Global Information Assurance Certification Paper

GIAC Level Two Firewalls, Perimeter Protection and VPN's Practical Assignment for Capitol SANS Version 1.4

December 10-15, 2000

Submitted by: Deepak Midha
01/06/2001

Assignment 1: Security Architecture - 25 Points

Define security architecture for GIAC Enterprises, a new Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings. 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).

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.

Introduction:

With the objective of defining a security architecture for GIAC Enterprise, a new Internet startup that expects to earn $200 million per year in online sales. It is presented and commented as below.
Design Infrastructure:

DMZ-1 This is equipped with array of web server and e-commerce server, which is for customer access to browse and purchase bulk online fortunes. This is a screened network.

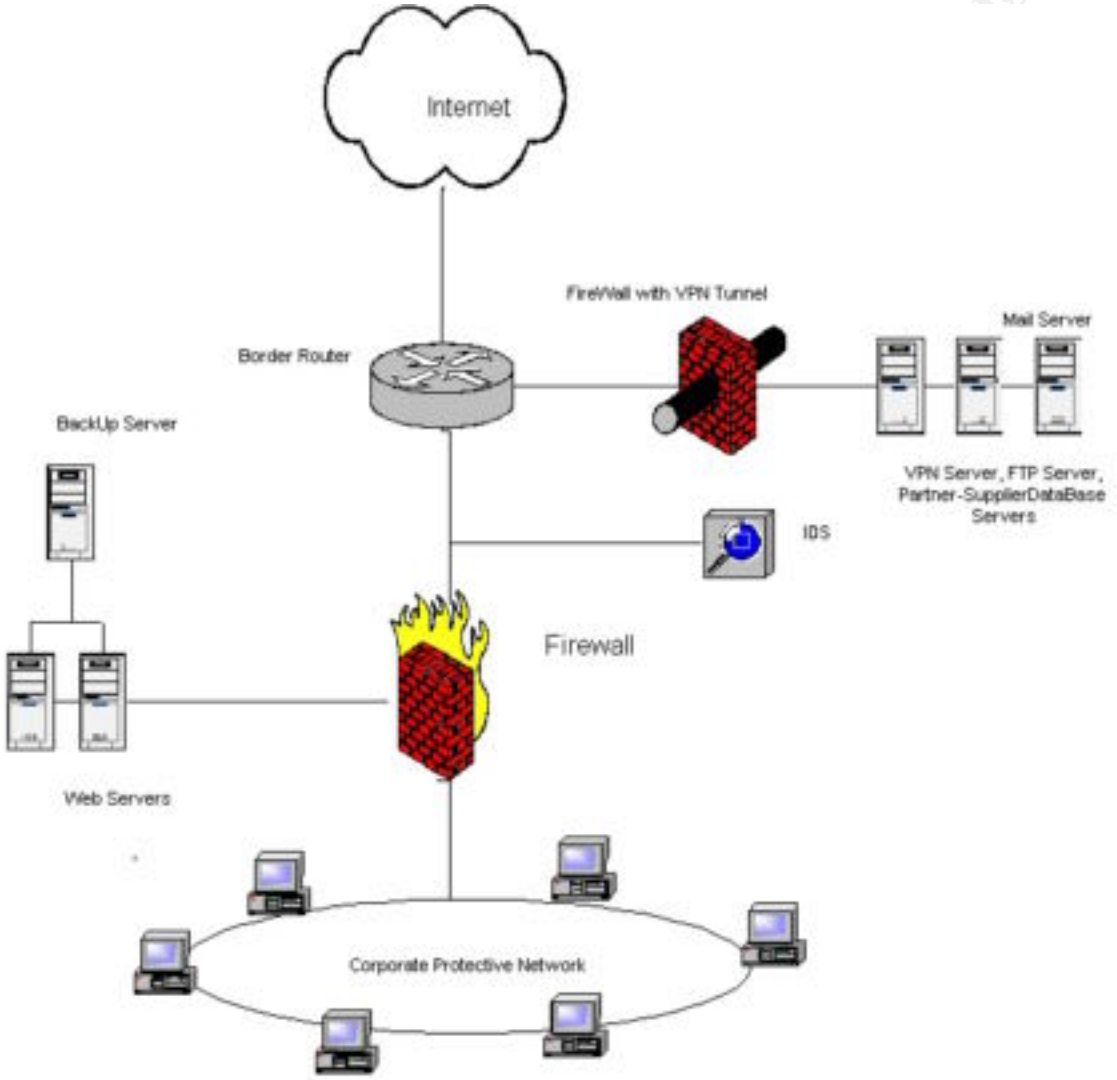
DMZ-2 This is equipped with VPN, E-mail, FTP, Database server etc. The main objective of this screened network is to allow partners and suppliers to access through VPN tunnel (encrypted data).

Corporate Protected Network: This is separated network and hosts only internal servers and workstations.

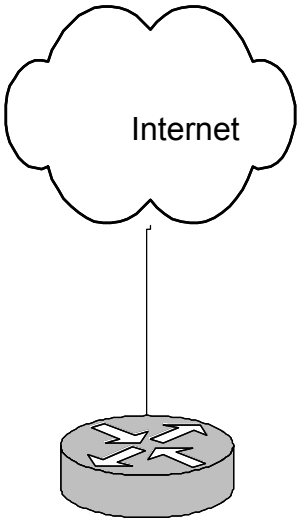
Adopting VISA's e-business partner requirements has created the baseline of secure design.
1-Firewall has been deployed at Internet entrance point.
2-Security patches are up to date.
3-IPSec is used to access database server from the Internet.
4-IPSec VPN Tunnel is used to send data across networks.
5-MicroTrend Virus scan on mail server and Norton Antivirus on each workstation.
6-Users or Groups to access only the data and machine they are authorize to.
7-Every user has its own password, which follows corporate password policy.
8-All user logins are logged included fail logins.
9-All hardware passwords are periodically changed.
10-The different tests are run regularly to check the integrity of security systems and processes.

In addition access to security devices are limited authorized personnel only. All logs are reviewed daily and kept for year. Security Policy is updated periodically.

GIAC Network design



Border Router:

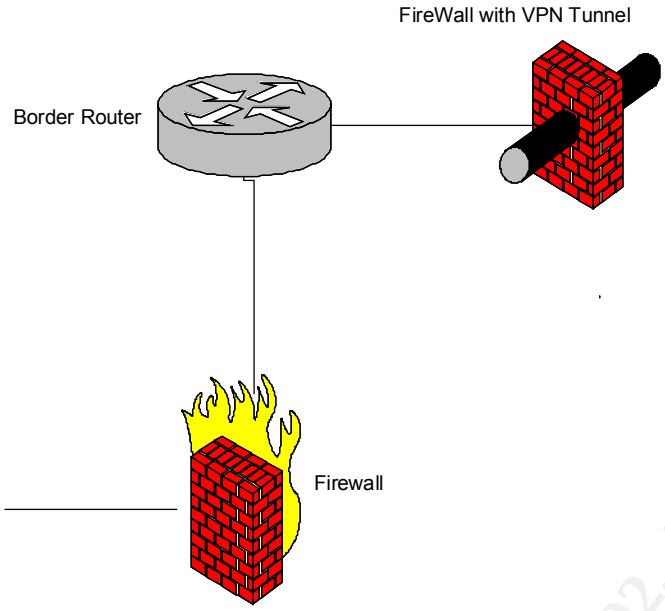


For this assignment, I used a Cisco 3640 router. Which is directly connected to the Internet. This is doing a basic filtering. Beside the use of firewalls, this Internet access router is configured to reduce the load of firewall by reducing the possibilities of DDoS attacks as well as will block the entrance of badly formed packets (Fragmentations, source route etc.). It will discard traffic that has no legitimate purpose coming into our network. While not representing the core of this security platform, it plays an important part in being a front line defense mechanism.

There are some basic rules to follow while configuring packet filtering.

- Set up an explicit default deny (with logging) so that you are sure that default behavior is to reject packets.
- Deny inbound traffic that appears to come from internal addresses (that is the indication of forged traffic or bad network configuration).
- Deny outbound traffic that does not appear to come from internal addresses (again such traffic is either forged or bad network configuration).
- Deny all traffic with invalid source addresses (including broadcast and multicast source addresses).
- Deny all traffic with source route or IP options set.
- Deny ICMP traffic over a reasonable size.

Firewalls:



There are two Cisco PIX Firewalls (515) been used in this architect for packet filtering. In order to reduce load as well as keep the different DMZ's separate. This PIX 515 comes with 16 MB of flash memory and 32 MB of RAM. The second one is equipped with VPN card.

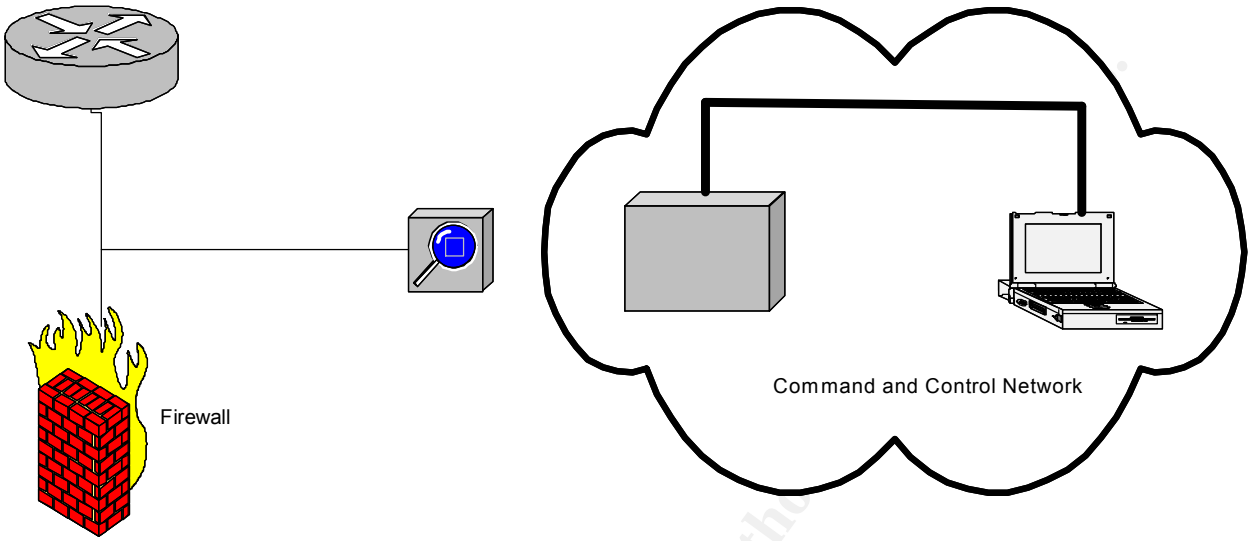
PIX firewall is considered for this design due to its outstanding features such as its ability to block ActiveX controls, implements Stateful control through the firewall, Protects inside systems from TCP SYN flood attacks (allows servers within the inside network to be protected from DOS attack), Port Address Translation (PAT), Utilizes IPSec technology, Encrypts data between peers works with VPN clients, certification authorities, routers etc are some of the various features.

The First one in this design has three interfaces with NAT. The first interface is connected to the Border Router and has public IP Address is accepting filtered traffic from the router. The second interface is connected to DMZ-1, Which has e-commerce, web servers for customer or employees from outside to browse through. Third interface is connected to Corporate Protected Network.

The Second PIX Firewall has two interfaces; first interface is connected to border router and second is connected to DMZ-2. The main purpose of this firewall is that is configured for VPN tunneling and IPSec traffic for Partners and suppliers to get to their Database and away from corporate network. The e-mail servers are running Trend Micro's Virus scan.

The firewalls are configured according to company security policy.

Intruder Detection System:

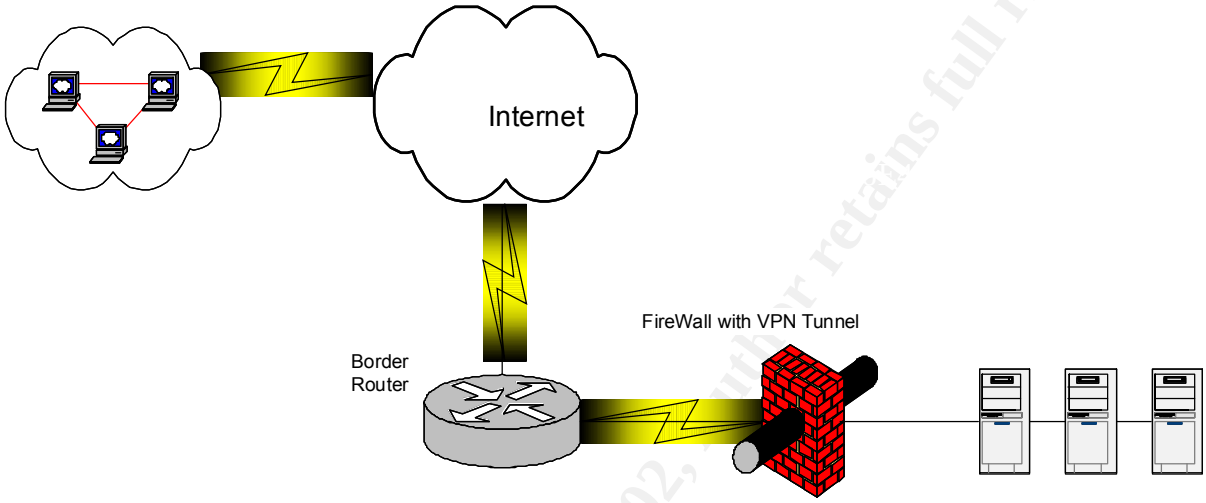


Firewalls do not guarantee the complete security of the network. It is necessary to introduce the Intrusion Detection System (IDS) in the network to detect possible intrusion attempts. In our architect it sits between router and firewall.

The main monitoring objective for this IDS is to identify and alarm scanning and attack preparation. Besides continually monitoring the network, IDS can be used to aid in the verification of the router filters and firewall security policies.

In this design Cisco Secure Intruder Detection Systems (IDS) is used in standalone mode. In this environment sensor sniffs traffic and forwards alarms to the Director. The sensor may be configured to respond to alarms with a TCP reset, or to start an IP session log.

VPN:



VPN is a way of employing encryption and integrity protection so that a public network (Internet) can be used, as it was a private network. That reduces the cost as well as it is much secure. The traffic is encrypted, integrity protected and encapsulated into new packets. Which are sent across the Internet to something which undoes the encapsulation, checks the integrity And decrypts the traffic.

IPSec is becoming the standard protocol used by VPN devices to communicate with each other. IPSec is actually a collection of protocols used to wrap around the data sent between two devices. The IPSec protocols are the Internet Key Exchange (IKE), Authentication Header (AH), and the Encapsulating Security Protocol. (ESP)

IKE is used to negotiate which encryption and authentication methods will be used between two IPSec devices and how long they will last. These negotiated methods between devices are called Security Associations (SA). After each device has been properly identified, either via a pre-shared key or public key exchange, the IKE negotiations begin.

IPSec supports two encryption or authentication modes: Transport and Tunnel. Transport mode encrypts/authenticates only the payload of the ip packet, leaving the header untouched. Tunnel mode encrypts/authenticates both the header and the payload giving the added benefit of protecting the real source and destination of the packet.

If the use of AH is negotiated during the IKE process the data transmission can be protected using these methods: data origin authentication, connectionless integrity and protection against replay attacks. Be aware that the data payload is not encrypted when using AH.

If ESP is negotiated, then the following security services are offered: payload encryption, data origin authentication, connectionless integrity, protection against replay attacks, and limited traffic flow confidentiality (using a padding feature).

We have used an integrated solution for VPN and firewall here. One nice feature of an integrated solution is good ACL control and no NAT problems. The position of the VPN on separate Screened network (DMZ-2) allow us to ensure this is the only service they have access to protecting the corporate network which includes financial data etc.

Assignment 2 - Security Policy (25 Points)

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

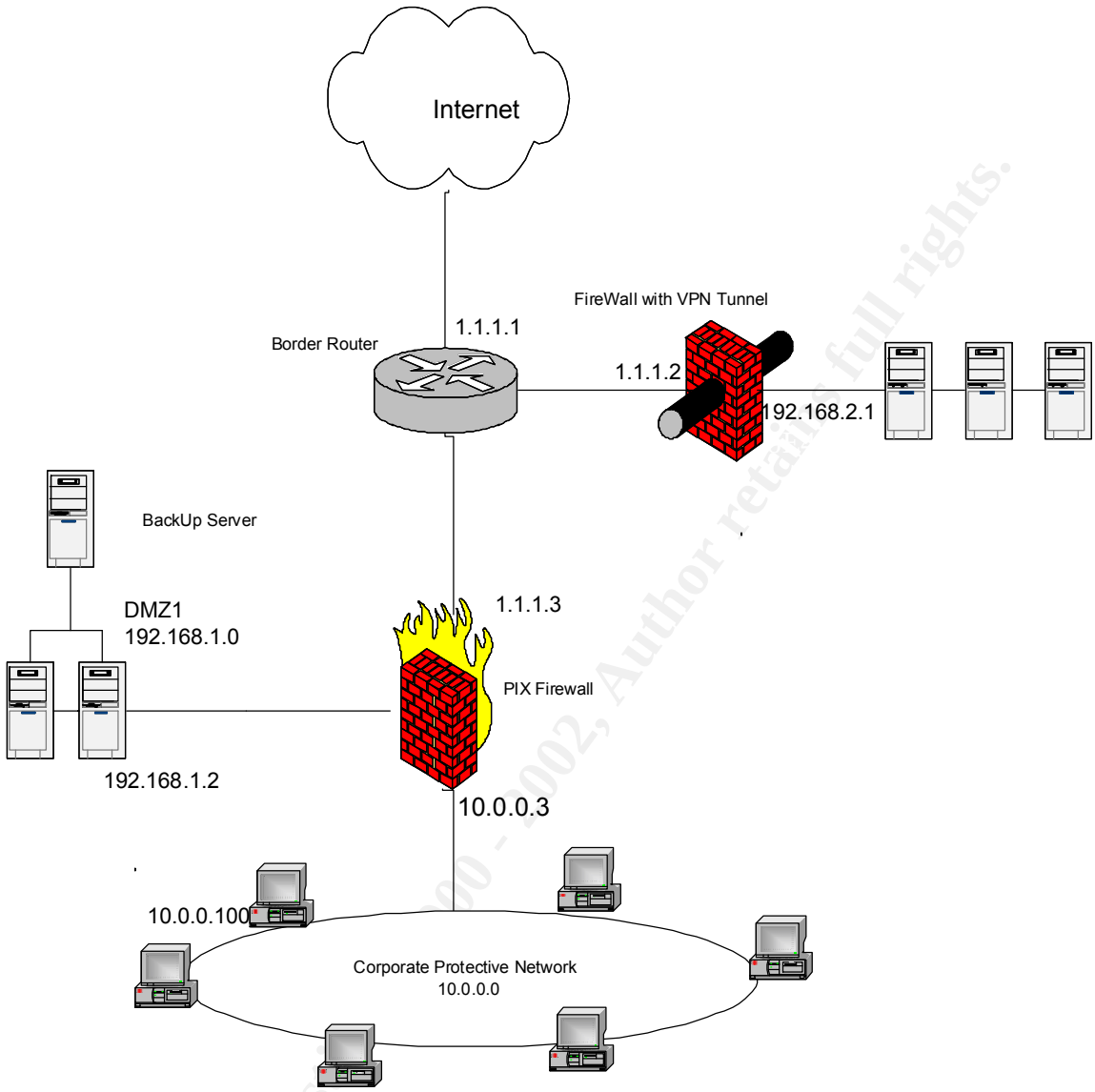
You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.
By 'security policy' we mean the specific ACLs, firewall rule set, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, 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:

1. The service or protocol addressed by the ACL or rule, and the reason these services might be considered vulnerability.
2. Any relevant information about the behavior of the service or protocol on the network.
3. The syntax of the ACL, filters, rule, etc.
4. A description of each of the parts of the filter.
5. An explanation of how to apply the filter.
6. 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.)
7. Explain how to test the ACL/filter/rule.

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

Introduction

This assignment consists in define an additional security policy based on our security architecture. For the definition of the filters to be implemented in the firewalls, it is necessary to specify the addresses of the involved sub-nets.
For this assignment we will discuss the Border router ACL's, PIX firewall configuration as well as IPSec policy for VPN access



Now lets look at some of the Cisco filter router configuration statement. I configured my 3640 Cisco router to block some of the services to discard illegitimate traffic.

I created extended access list (100).
! for anti-spoofing, block private RFC1918 addresses.

access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 172.16.0.0 0.15.255.255 any
access-list 100 deny ip 10.0.0.0 0.255.255.255 any

!block loopback address

access-list 100 deny ip 127.0.0.0 0.255.255.255 any

To harden router and stop Eavesdropping and session Replay. I also added these additional commands in configuration.

From the interface configuration mode.
!disable the source routing
no ip source-route
!disable the sending of redirect messages
no ip redirects
!disable the generation of ICMP unreachable messages
no ip unreachables
!disable fast switching and autonomous switching
no ip route-cache
!disable multicast route caching
no ip mroute-cache
!disable the maintenance operational protocol (MOP)
no mop enabled
!disable cisco discovery protocol. This could be from interface or global mode
no cdp run
no cdp enable
!disable proxy arp
no ip proxy-arp
!disable eco, finger replies
no service finger
no service tcp-small-servers
no service udp-small-servers

Block SNMP from the outside

Access-list 100 deny udp any any eq snmp

To log every event on the Perimeter (Border) router to the sys log server. This is optional, this could create long log files. Is this really needed?

Logging trap debugging
Logging x.x.x.x !IP address of syslog server

There are some other things we can block.i.e.

Linuxconf is a program that has both a graphical client and a remote web based management interface to allow administrators to easily configure many aspects of a Linux server. Scans for this may be an attempt to simply identify Linux based servers in an effort to launch an unrelated attack on a different exploit. Or, someone may be sitting on a Linuxconf exploit that the rest of us don't know about yet. Either way, using linuxconf over insecure networks is not recommended due to the plain text nature of the protocol and should be restricted to internal hosts only, or disabled if not needed.

!block Linuxconf:
access-list 100 deny tcp any eq 98

Klogind is the Kerberos authentication daemon. Buffer overflows have been found in some version 5 klogind daemons. We can insure any servers we have using Klogind are up to date, but if we aren't using the service it's best just to filter it at the perimeter.

a*ccess-list 100 deny tcp any eq 543*

SGI Objectserver is a daemon that provides sys admin functions under Irix versions 5.3 to 6.2. Newer versions do not utilize this daemon. Since we have no older Irix machines, this does not affect our network. However, for sake of completeness, here is the ACL:

access-list 100 deny tcp any eq 5135

Mountd is used by NFS and some versions are vulnerable to exploits. We can block it with:

access-list 100 deny tcp any eq 635

NetBus and Back Orifice are remote admin hacks for Windows based machines. If someone manages to slip one of these by our perimeter in the form of a trojan, we don't want to make it easy for them to connect. We have a problem however, since these utilities are both configurable to run on any arbitrary port. We should still block the most commonly found (default) ports, and watch for suspicious traffic on other ports.

access-list 100 deny udp any eq 31337
access-list 100 deny udp any eq 12345
access-list 100 deny udp any eq 12346
access-list 100 deny udp any eq 20034

Talk and Ntalk are unix daemons used for sending messages between users on the same or different machines. We don't have a business requirement for them, so it represents a potential threat. Disable via:

access-list 100 deny udp any eq 517
access-list 100 deny tcp any eq 517
access-list 100 deny udp any eq 518
access-list 100 deny tcp any eq 518

Ircd is the server daemon for the Internet Relay Chat network. Again, since we have no business requirement, we should block it.

access-list 100 deny tcp any eq 6667
access-list 100 deny udp any eq 6667

SWAT is the Samba Web Admin Tool. It runs via a web browser and allows an administrator to configure SMB shares on Unix and Linux machines. While SWAT does allow for authentication, we don't want intruders to be able to try to poke holes in it. We can block it via:

access-list 100 deny tcp any eq 901

Bootp, the precursor to DHCPD allows for automated configuration and booting of network clients. We don't want to see that traffic coming into our network from outside.

access-list 100 deny tcp any eq 67
access-list 100 deny udp any eq 67

XDMCP is the management protocol for X Windows. Our basic security policy blocks X Windows connections, and we should also prevent unauthorized external parties from communicating with our hosts listening to xdmcp requests. We can block it via:

access-list 100 deny tcp any eq 177
access-list 100 deny tcp any eq 177

RIP is an older routing protocol still commonly used in many network devices. We don't want anyone outside to have the ability to confuse our routers, so we block it.

access-list 100 deny udp any eq 520

LDAP is the Lightweight Directory Access Protocol. Allowing unauthorized external users access to our directory is giving up far more information that we wish to allow.

access-list 100 deny tcp any eq 389
access-list 100 deny udp any eq 389

One very important note is that on a Cisco router we need to end our ACL with the following rules (after entering in the Base policy listed in the Question, along with the additional rules I list above):
access-list 100 permit tcp any any
access-list 100 permit udp any any

If we forget these entries then ALL traffic will be denied because of the implicit 'deny all' at the end of each Cisco ACL. The ACL should be applied on the external serial interface in the in-bound direction:

interface serial 0/0
ip access-group 100 in

These commands were applied to the serial port of the router in the inbound direction.

Let's look at the firewall. The first one with three interfaces and the following attribute.

- Address translation is performed between the interfaces.
- Web servers on DMZ-1 are publicly accessible for customers.
- The corporate network has private addresses (10.0.0.0), The DMZ-1 interface has addresses (192.168.1.0) and outside network has legal registered addresses (1.1.1.0)
- TCP and UDP from the corporate network are allowed to go out on DMZ-1 and outside
- Administration has telnet access to PIX Firewall console.

Lets assume the Network has following IP addresses and network masks.

- Outside network interface address 1.1.1.3 mask 255.255.255.0
- Inside network interface address which is connected to corporate LAN 10.0.0.3 mask 255.0.0.0
- Interface connected to DMZ-1 192.168.1.1 mask 255.255.255.0

The following rules will work on PIX running version 5.0(1) or higher

PIX firewall provides *nameif* and *interface* command statements for the interface in the default configuration.
#Give the interfaces symbolic names to make the config easier.

nameif ethernet0 outside security0
nameif ethernet1 corporate security100
nameif ethernet2 dmz1 security50

interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto

#Assign and identify the IP Addresses of each of the three interfaces
ip address outside 1.1.1.3 255.255.255.0
ip address corporate 10.0.0.3 255.0.0.0
ip address dmz1 192.168.1.1 255.255.255.0

#Specify the name for the PIX Firewall. This name appears in command line prompt.

hostname giacfirewall

#Disable the RIP attributes. You do not want to route.

no rip corporate passive
no rip outside passive
no rip corporate default
no rip outside default

Set the outside default route to the router attached to the Internet.

route outside 0.0.0.0 0.0.0.0 1.1.1.1 1

#Give telnet access to administrative host to PIX firewall console.

telnet 10.0.0.100 255.255.255.0

#Let corporate users start connections on the DMZ1 and outside interfaces

nat (corporate) 1 10.0.0.0 255.0.0.0

#Give the IP Address of web server a name. We call it GIACwebserver.

name 192.168.1.2 giacwebserver

#Let any user from the outside access the webserver

conduit permit tcp host giacwebserver eq 80 any

Lets take a look at the other PIX VPN/Firewall

#Assign the names to interfaces.

nameif ethernet0 outside security0
nameif ethernet1 dmz2 security100

interface ethernet0 auto
interface ethernet1 auto

#Assign the IP Addresses to the network interfaces.

ip address outside 1.1.1.2 255.255.255.0
ip address dmz2 192.168.2.1 255.255.255.0

#Assign the virtual IP Addresses for access by remote VPN clients.

ip local pool dealer 172.16.1.1-172.16.1.254

#The static command statement maps outside interface IP Address to the servers on the DMZ2.

static (dmz2,outside) 192.168.2.0 192.168.2.0 netmask 255.255.255.0

#The *sysopt* command statement specifies that IPSec *static* command statement is trusted.

sysopt connection permit-ipsec

#Establish the encryption policy for ISAKMP.

crypto ipsec transform-set strong esp-des esp-md5-hmac
crypto map ipsecin 5 ipsec-isakmp dynamic cisco
crypto map ipsecin client configuration address initiate
crypto map ipsecin client configuration address respond
crypto map ipsecin interface outside

#Establish the ISAKMP policy.

isakmp enable outside
isakmp key cisco123 address 0.0.0.0 netmask 0.0.0.0
isakmp client configuration address-pool local dealer outside
isakmp policy 10 authentication pre-share
isakmp policy 10 hash md5

Order in Which You Configure Your IPSec

TIPS: If you will implement interoperability with a CA, Cisco recommends that you perform your IPSec configuration in the following order:

1. CA
2. IKE
3. IPSec
4. IKE Extended Authentication---applies only if you are configuring user authentication for remote VPN clients
5. IKE Mode Configuration---applies only if you are configuring dynamic IP addressing for remote VPN clients

If you will not implement interoperability with a CA, and you will implement IKE, Cisco recommends that you perform your IPSec configuration in the following order:

1. IKE
2. IPSec
3. IKE Extended Authentication---applies only if you are configuring user authentication for remote VPN clients.
4. IKE Mode Configuration---applies only if you are configuring dynamic IP addressing for remote VPN clients.

Assignment 3 - Audit Your Security Architecture (25 Points)

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Border Router and 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.

1. Implement the assessment. Validate that the Border Router and Primary Firewall are 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.
2. 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.

1. Assessment plan

An audit is a process of review to identify configuration errors in the environment. The goal is to identify as many risks as possible and then to eliminate those risks.

Here is the approach I recommend:

- Begin with a baseline of normal activity, which can be gathered from the on-site technician, and from viewing the event logs.
- Identify the operating system levels and patch levels across the company's environment. Consistent software revision levels make an attacker's job more difficult (it limits the exploits available to him), and the company's technician's job easier (with fewer revision levels to consider, it is easier to focus on and act on relevant security alerts).
- Identify those staff members who have dedicated Information Security responsibilities.
- Gather all relevant documentation (such as Security Policy, Security Procedures Document, Firewall configuration document, Firewall procedures document, Network diagrams, and Employee handbook).
- Arrange a suitable time to carry out the audit. Although network analysis tools can create performance problems if run at peak times, it is important to have access to the on-site personnel, so the audit is likely to be carried out during normal business hours.
- The costs of performing the audit. Three days is enough to identify a task list of urgent things to attend to. It is prudent to budget for two people one should be outside the company, if possible. I would say approx $1000 a day for the outside consultant.
- Get agreement from the on-site IT staff to have a closing meeting to discuss the results, and then for the on-site staff to follow up any outstanding points, e.g. investigate unexplained open ports.
- Identify the risks in performing the audit, and communicate these risks to management at the company. Vulnerability scanning tools can have unpredictable results, e.g. a Denial of Service (DOS) attack against the company itself. Network performance may be negatively affected by audit tool activity. Password cracking tools may violate user privacy. It is important to get written approval for the audit from the company's management before beginning any work.

2. Implement assessment

To confirm that the firewall & perimeter (border) router are actually implementing the security policy, there are different tools can be used to perform these tests. For example intrusion analysis tool such as Nmap, NetXray, Network sniffer etc.

Let's look at Nmap tool.

To determine which TCP ports of your firewall are filtered, you have several options with nmap. You can try the Stealth Scan option, such as "-sS" or "-sF" (NOTE: Test stealth scanning on a test remote host first. Some systems panic/crash from stealth scan). Stealth scanning is an option some blackhats use in attempt to obscure their activities. By using this scanning method, not only can you test your firewall rule base, but also you can verify if your firewall logs can detect the stealth scans (FW-1 ver 4.x should detect all nmap stealth scans). Another option I like is "-g", which lets you set the source port. You can test for misconfigured rules that allow packets based on source ports, such as ftp data (port 20), dns lookups (port 53) or return http traffic (port 80). Notice how in this scan I am scanning all 65,000 possible ports. This will take a long time, around 60 minutes. However, it is thorough.

```
midha #nmap -v -g53 -sS -sR -P0 -O -p1-65000 -o nmap.out victim6
Starting nmap V. 2.52 by dmidha@comcastbusiness.com
Initiating SYN half-open stealth scan against victim (192.168.1.2)
The SYN scan took 4086 seconds to scan 65000 ports.
Initiating RPC scan against victim (192.168.1.2)
The RPC scan took 2 seconds to scan 65000 ports.
For OSScan assuming that port 21 is open and port 22 is closed and neither are firewalled
Interesting ports on victim (192.168.1.2):
(The 64985 ports scanned but not shown below are in state: filtered)
Port       State      Service (RPC)
21/tcp     open       ftp
22/tcp     closed     ssh
23/tcp     closed     telnet
25/tcp     closed     smtp
53/tcp     closed     domain
79/tcp     closed     finger
80/tcp     open       http
109/tcp    closed     pop-2
110/tcp    closed     pop-3
111/tcp    closed     sunrpc
143/tcp    closed     imap2
443/tcp    open       https
512/tcp    closed     exec
513/tcp    closed     login
514/tcp    closed     shell
```

The results here show of the 65,000 ports scanned, 64985 are filtered, leaving 15 of them not filtered. A this point we are not concerned whether the 15 ports are opened or closed, we only want to determine which ports were not filtered. In other words, these 15 packets were able to pass through the firewall. You can now take this information and compare it to your firewall rule base.

I would recommend and use commercial scanner: ISS Internet Scanner.

This scanner uses profiles to configure which tests to perform. There are two key dimensions to the security audit:

A- Verify that there are no configuration errors in the environment, i.e. make sure that certain traffic is actually being blocked if everyone thinks that it is being blocked.
B- Suggest ways to improve the current configuration based on industry best practice and an analysis of the audit logs.

I would create an ISS Internet Scanner profile to test the existing configuration: a level three NT scan with both Brute Force and Denial of Service options turned off. Using the Brute Fore option can lead to accounts being locked out. It would be equally unpleasant if Denial of Service attacks succeeded during heavy business hour.

Once you have identified what resources can be accessed with your port scanner, you can dig deeper. As discussed above, there are a variety of methods and tools to digging deeper. All of these tools are shareware/freeware, so no excuses. Here are several of my favorites.

Nessus (runs on Unix, client can run on 95/NT)	I consider one of the best, free vulnerability scanners.
Whisker (runs on anything that has PERL)	Searches websites for vulnerabilities
Hping2 (runs on Unix)	Build your own ICMP/TCP/UDP packets.
Winfingerprint (runs on 95/NT)	Enumerates NetBIOS Shares, Users, Groups, and Services
legion (runs on 95/NT)	From the guys at Rhino9, scans for smb shares
Sam Spade (runs on 95/NT)	Similar to WS Ping ProPack, but with some different goodies

3. Perimeter analysis

Our perimeter security implementation as laid out in this design and as describe depends on the Firewall Rule base being correctly configured. We would expect to see no surprises from this analysis. We should be up to date with all the patches and security policies.
The perimeter defense, and it also depends on the IT staff making the necessary changes to protect against new vulnerabilities.
This is not to say there are no causes for concern or places where improvements could be made. By using a different vendor for our VPN solution, as compare to integrated solution, will result in added security but will be hard to configure. Solution does rely heavily on the Cisco PIX firewalls and Cisco border router. Should an exploit be exposed in the PIX, our internal corporate network would be vulnerable.
For the added cost of complexity, a good way to guard against this type of scenario is to implement a layered approach, with firewalls from different vendors for example proxy application firewall with web caching sitting between our corporate network and the Internet. This approach adds cost (more hardware), complexity and troubleshooting even more difficult

But the odds of someone finding an exploit for two totally different firewall architectures at the same time before you have the chance to plug either hole is slim.
A sample of this type of layered approach can be seen in the following

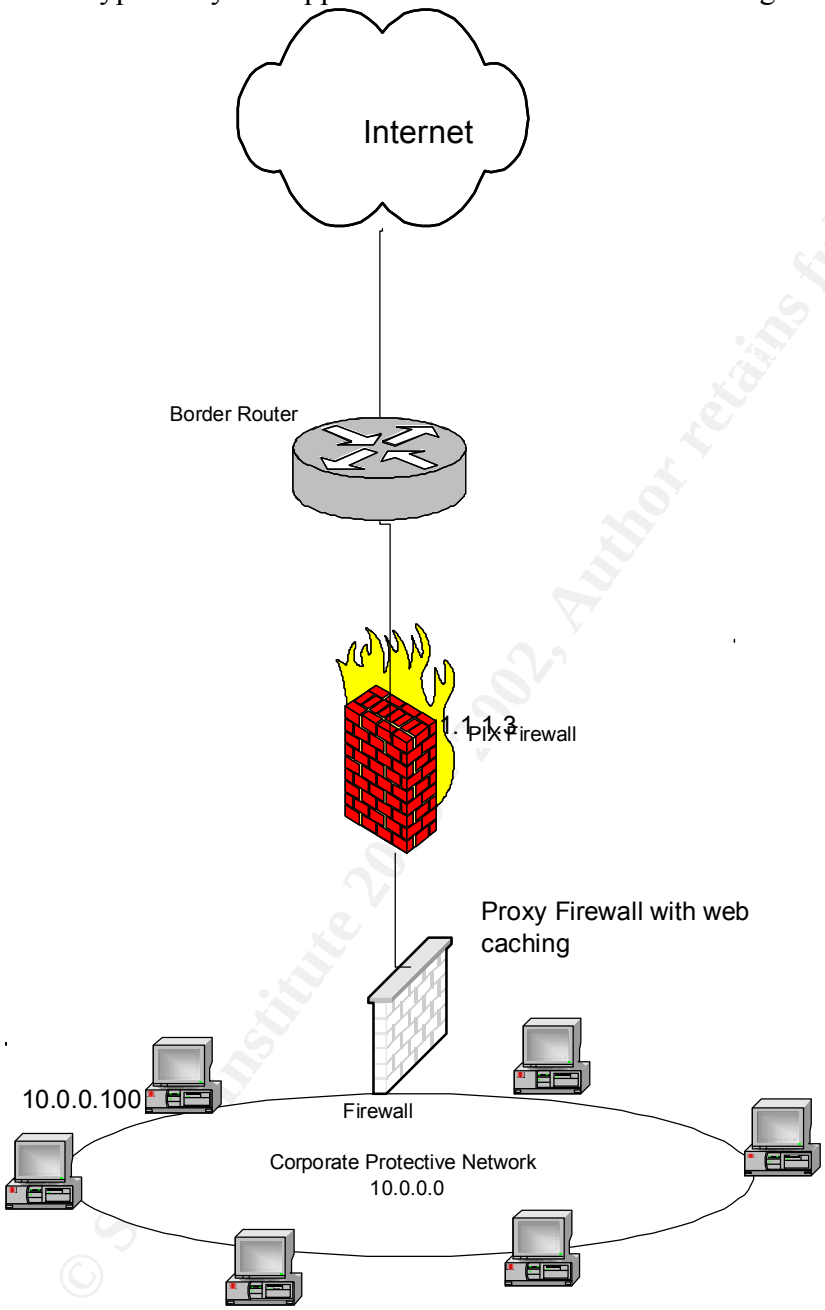


diagram:

Using a 'defense in depth' approach, I would recommend that

- Employee awareness of security is raised.
- Proper training

- A hardware support contract is arranged, so that should the firewall or border router need to be serviced, a replacement could be provided within an agreed amount of time, and the business' revenue would not be jeopardized.
- There is a weekly review of the Firewall logs to ensure that the Rule base is behaving as expected, and to look for patterns of suspicious activity.

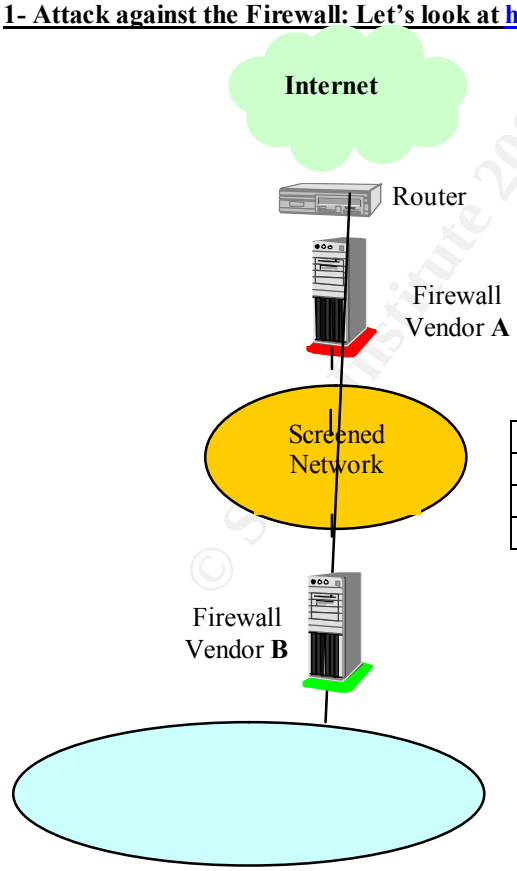
Assignment 4 - Design Under Fire (25 Points)

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 http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. 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.
2. 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.
3. 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.

1- Attack against the Firewall: Let's look at http://www.sans.org/giactc/gcfw.htm)/frank_meylan_11-18-00



Sample Configuration	
Router	Cisco 7000
Firewall Vendor **A**	Checkpoint Firewall -1
Firewall Vendor **B**	NAI Gauntlet

As per diagram above created by Frank_Meylan. He chose to use Checkpoint firewall-1. Which has a known vulnerabilities (exploit):

Exploit
Most frag based attacks that use incomplete or illegal fragments will work, Including jolt2. The firewall does not have to be attacked directly, if the frags are routed through the firewall for a system behind the firewall, FW-1 is still taken out.

Reason
FW-1 does not inspect, nor does it log, fragmented packets until the packet has first been completely reassembled. Since these exploit packets are never fully assembled, they are never inspected nor logged. Thus, the firewall's own rule base cannot be used to protect against the attack.

The actual CPU utilization is most likely the result of the application attempting to reassemble hundreds or thousands of incomplete and illegally fragmented packets. As stated above, the firewall rule base cannot block these packets, as they are never inspected.

Other firewalls may have the same problem and vulnerability.

Symptoms
CPU mysteriously hits 100% utilization, system locks up. Some systems may also crash, depending on OS type.

Solutions
Checkpoint has developed a short-term solution to the problem. A Percentage of CPU utilization is due to console error messages on some Unix systems. By disabling FW-1 kernel logging, some CPU utilization will be saved. However, all FW-1 kernel logging is disabled, you will have no capability for logging any firewall kernel events. At the command line on the Firewall, type as root:

fw ctl debug -buf

Ensure the operating system has the latest patches. Most operating system have recently released patches that help protect against fragment attacks.

Run an IDS module (such as snort). When you detect frag attacks block the source at the router (remember, the firewall CANNOT stop the attack, its rule base is powerless). However, this method may not work with spoofed Source packets.

2-Denial of Service attack and counter measures.

As we all know a typical cable modem network is a big-shared network. There is lot of broadcast and multicast taking place. There are lots of vulnerabilities and exploits can be done. Lets take a look how a DoS attack can take place and how to avoid it.

A typical DDoS attack takes the following form. A hacker breaks into several remote systems located on various networks. In this case 50 different cable-modem and DSL systems. A client program, which has the ability to generate packets. Using spoofed address can use this site as Broadcast Amplification site or typical DOS attack by flooding TCP, SYN, UDP and ICMP.

These two steps can significantly reduce the threat posed by DoS Attacks

- Egress Filtering to Stop Spoofed IP Packets from Leaving Your Network
- Stop Your Network from Being Used as a Broadcast Amplification Site

Egress filtering has been demonstrated as an effective tool to reduce the possibility of local network entities being used to support a distributed denial of service (DDoS) attack against a third party. To understand how egress filtering works, it is important to understand the methods used in creating these attacks.
Ensure that router and firewalls are configured to forward IP packets only if those packets have the correct Source IP Address for your network. The correct Source IP Address (es) would consist of the IP Network Addresses that have been assigned to your site. It is important to do this throughout your network, especially at the external connections to your Internet or upstream provider.

All organizations connected to the Internet should only allow packets to leave their network with valid Source IP Addresses that belong to their network. This will minimize the chance that your network will be the source of a *Spoofed* DoS Attack. This will *not* prevent Distributed DoS attacks coming from your network with valid source addresses.

The following is a list of source addresses that should be filtered.

0.0.0.0/8 - Historical Broadcast
10.0.0.0/8 - RFC 1918 Private Network
127.0.0.0/8 - Loopback
169.254.0.0/16 - Link Local Networks
172.16.0.0/12 - RFC 1918 Private Network
192.0.2.0/24 - TEST-NET
192.168.0.0/16 - RFC 1918 Private Network
224.0.0.0/4 - Class D Multicast
240.0.0.0/5 - Class E Reserved
248.0.0.0/5 - Unallocated
255.255.255.255/32 - Broadcast

If you are using Network Address Translation (NAT), you need to make sure that you perform this filtering between your NAT device and your ISP, and you should also verify that your NAT device configuration only translates address used and authorized for your internal address space. Denying Private and Reserved Source IP Addresses can be accomplished with filtering on routers, firewalls, and hosts

Ensure that your network cannot be used as a Broadcast Amplification Site to flood other networks with DoS attacks such as the "smurf" attack.

Configure all of your systems (routers, workstations, servers, etc.) so that they do not receive or forward Directed Broadcast traffic.

3-Attack plan to compromise Internal network reason for choosing host

Attack plan would consist of probing the network and look for open ports. There are few week links in the internal network, which can be compromised for example FTP server. This is usually not hardened and secured properly. Most of the commercial sites use FTP service and usually ports 20,21 are open in the perimeter firewall. These FTP services are usually setup to log in as "anonymous" user. Which then asks for password and expected to enter his or her e-mail address in response. At most sites this request in not enforced and user can enter whatever they want, as long as it looks like an e-mail address. Many standard ftp servers usually shipped with Unix version do not even log this information.

Once the connection is made, it could be used to compromise these anonymous FTP areas. This can be used to distribute illegal data. Which in fact consumes resources, such as disk space and network bandwidth (mainly on Internet connection). It interferes with legitimate use of these resources: It's a denial of service attack.

This data could be illegal, pirated stuff etc. Which could bring the site to legal actions for assisting or could generate significant negative publicity.