GIAC Enterprises
GCFW Practical Version 1.6

Jana Dunn

INTRODUCTION

Submitted in partial fulfillment of the requirements for the GCFW certification, this document describes a proposed security architecture for GIAC Enterprises (GE), a fictitious, on-line, business-to-business vendor of fortune cookie fortunes.

GIAC Enterprise's security architecture is designed to meet its business needs while securing company information assets.

GIAC ENTERPRISES' NETWORK ACCESS NEEDS

Customers: GE's primary customer base purchases fortunes in bulk online. Customers need secure access for their financial transactions and for receipt of the product.

Suppliers: GE purchases fortunes from fortune cookie authors external to the company. These suppliers require a secure method for uploading their products to GE.

Partners: GE has international business partners that translate and resell fortunes; they need to be able to download bulk fortunes for translation and to upload the translated fortunes to GE. Both of these transactions need security.

Electronic mail: GIAC Enterprises' staff members need to be able to receive and send mail to and from partners, suppliers, customers, and other GE staff members. GE customers, suppliers, and partners need to be able to send electronic mail to GE staff members.

Staff access: GIAC Enterprises' staff members needs to be able to read and send electronic mail when they are away from the office. In addition, networking staff has requested that there be a secure way they can reach console ports on servers, routers, and switches from outside the office.

ARCHITECTURE

The following describes the elements of GE's perimeter defense, starting from the edge of the network and moving in.

GE's security architecture is designed to separate services and servers according to the access needs of the users of those services.

Basic Packet Filtering at the Border Router
GE has selected a Cisco 3620 as its border router. This router provides basic ingress traffic filtering, blocking traffic from the Internet with spoofed or illogical source addresses. Providing this service at the border router reduces the load on the main firewall. The IOS version is 12.0.9, the latest General Deployment version of IOS IP available for this router model as of this writing.

Main Firewall
GE has selected a Cisco PIX 515-UR as its main firewall. GE has this selected this PIX model for its support of multiple interfaces (up to six interfaces). This model also supports failover, should GE decide to add a redundant firewall in the future. The firewall is using PIX IOS version 6.0(1.101).

The PIX is the security workhorse in this design; its primary job is to block hostile traffic from the Internet. All connections to and from the Internet traverse this firewall. In addition to the firewall's primary Internet-traffic-blocking duties, the PIX also provides the following functionality:

NAT (network address translation): GE uses private IP addresses for machines on its internal corporate and service/perimeter networks. The PIX will provide NAT for outgoing connections from internal hosts and also for connections from more-secure networks to less-secure perimeter networks.

Mail Proxy: The PIX MailGuard function provides a mail proxy feature for incoming electronic mail destined for GE's corporate mail server; the corporate mailserver is on a network internal to the firewall. MailGuard logs SMTP activity and allows only a minimal set of SMTP server commands.

VPN Termination: The PIX firewall also serves as a VPN server; this is where VPNs used by partners and suppliers terminate. Partners and suppliers will be provided with Cisco VPN 3000 Client V3.0 software. This client software version requires version 6.0 (or greater) IOS on the PIX firewall.

Perimeter Networks: In addition to the firewall's "outside" connection (to the border router) and its inside connection (to the internal corporate networks), the firewall also provides connectivity for a number of service (perimeter) networks. All perimeter networks are switched; the switches are Cisco 2924XLs and Cisco 2912XLs. All hosts on perimeter networks have been hardened with appropriate tools, with unneeded services turned off. Each perimeter network has its own backup server and IDS system. GE security policies and procedures include procedures for keeping servers, firewalls, and network equipment and their configurations up-to-date with regards to patches, software versions, vulnerabilities, and anti-viral software.

Customer DMZ: This network provides services for customers who purchase bulk fortunes. Customers use a web-based interface for their interactions with GIAC Enterprises; SSL provides security for their transactions. Customers do not have network access to any servers or services on any of the other portions of GE's network. The GE mail server also resides on this network. The mail server provides secure, web-based email using SSL. Incoming mail is scanned for viruses; the virus signatures will be kept up to date; the networking staff has established a procedure for handling this. The DNS server will contain name/address mappings for the customer-accessible services: the web server and the mail server. Hosts on this network can not initiate connections to the internal networks and have limited access to services on the other perimeter networks.

Partner/Supplier Service Network: GE's partners and suppliers will connect to GE's network using VPNs to provide secure data transfer. Once connected, the VPN clients will have access to this service network. To pick up or deliver a fortune cookie file, a partner or supplier connects using VPN software, authenticates via the RADIUS server, then connects to and authenticates at the FTP server. On the FTP server the partner or supplier has designated locations where he can pick up or drop off files. The servers on this network can not initiate connections to the internal networks; any connections to these servers (for example, to upload a fortune file from the internal database) are initiated from the internal networks. The RADIUS server on the network services network provides authentication for the VPN clients. The DNS server on this network contains an entry for the partner/supplier FTP server, also on this segment. It also functions as a general DNS server for VPN clients when they are connected via their VPNs; it makes recursive queries to Internet-based servers for the clients. This DNS server does not contain entries for other perimeter or internal GE servers. VPN users will not have access via the VPN to internal networks; they will not have access via the VPN to other perimeter networks. Hosts on this network will have restricted access to other perimeter networks.

Network Services Network

The network services network also connects to the primary firewall. Here reside those services required by nearly all the GE subnets: an internal DNS server, an authentication server for router, switch, and VPN access, a boot and configuration server for network devices, a SQL*Net proxy server, an SNMP-based monitoring station, and a logging (syslog) server.

Secure Remote Access for Staff

For networking staff access from offsite, GE will provide a console server with a secure (passworded) dial-back modem attached. Systems connecting via this modem and console server will not become network nodes (i.e. no PPP access); this setup is only to allow out-of-band access to console ports. This will be the only modem allowed behind the firewall. Only servers and devices managed by the networking staff will be connected to this console server. While in the office, the networking staff may access the console server via their local network; access is authenticated.

Internal Networks and the Internal Firewall

The primary firewall provides the first layer of protection for the internal networks. No hosts or services on any of the perimeter networks or on the Internet are allow to directly initiate a connection to the internal networks with the exception of the SQL*Net proxy server, which must communicate with the database server on the internal database network. Any hosts or services that require access from a perimeter network or from the Internet should be placed on one of the service/perimeter networks. In addition to the primary firewall, the GE security architecture allows for additional protection and separation of internal resources via an internal firewall.

The GE internal network defenses mirror the design of the main perimeter defenses. A Cisco Catalyst 5000 switch provides the central connectivity; an RSM (Route-Switch Module) in the Cat5k provides routing between the networks. GE has selected an IOS version for the RSM that includes Cisco Secure Integrated Software (formerly the Firewall Feature Set) to provide internal access control. GE selected the Cat5k/RSM/FW combination with flexibility in mind—the networking staff can create as many separate VLANs/networks as necessary to meet changing business needs, and the integrated firewall software allows the staff to construct appropriate security for these networks.

The systems containing the fortune database and the customer information database reside on an internal corporate network. The internal firewall limits access to this network. The customer webserver must interact with these databases; Customer Care may have a need to make some queries to these databases via SQL*Net. System and database management for these servers are to be conducted from workstations on the database server network.

Denial-of-Service Protection from the ISP

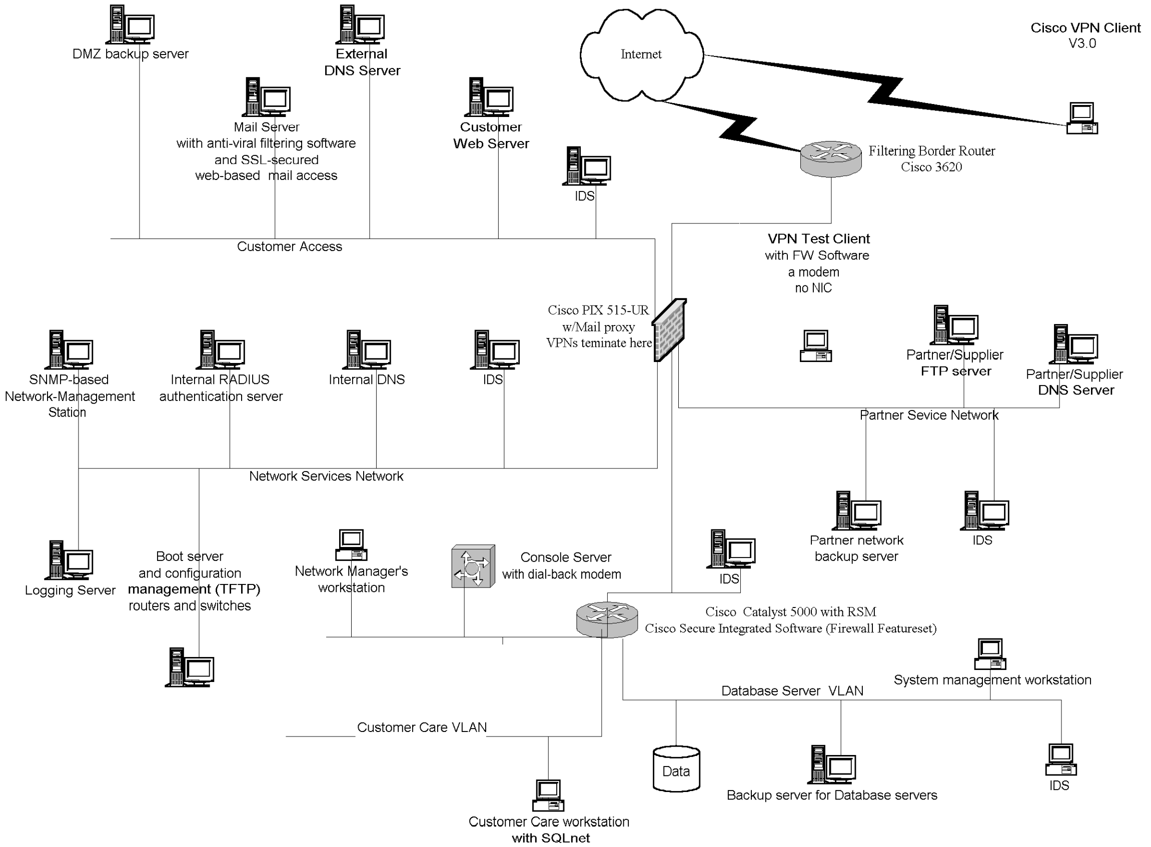
GE's ISP has recently begun offering Denial-of-Service protection. GE has contracted with the ISP for this protection.

ARCHITECTURE DETAILS

IP address assignments for the networks are as follows:

Network Name	Network Number or Address Range	Connects to	Default Gateway
Outside	195.195.195.0/24	195.195.195.1 (3620 router) 195.195.195.2 (Primary PIX FW)	195.195.195.1
PAT address, to Internet	195.195.195.33	Defined in Primary FW	N/A

Customer DMZ NAT Pool and PAT overflow	10.1.2.1.100 - 10.1.2.199; 10.1.2.200 PAT	Defined in Primary FW	N/A
Partner/Supplier Network NAT Pool	10.1.3.100 – 10.1.3.199; 10.1.3.200 PAT	Defined in Primary FW	N/A
Network Service NAT Pool	10.1.4.100 – 10.1.4.199; 10.1.4.200 PAT	Defined in Primary FW	N/A
VPN Pool	10.1.8.0/24	Defined in Primary FW	N/A
Customer DMZ	10.1.2.0/24	Primary FW	10.2.1.1
Partner/Supp. Net	10.1.3.0/24	Primary FW	10.1.3.1
Network Svcs. Net	10.1.4.0/24	Primary FW	10.1.4.1
FW Inside	10.1.1.0/24	Cat5K, Primary FW	10.1.1.1 (FW)
Network Mgmt. Net	10.1.5.0/24	Cat5K	10.1.5.1 (RSM)
Database Server	10.1.6.0/24	Cat5K	10.1.6.1 (RSM)
Customer Care	10.1.7.0/24	Cat5K	10.1.7.1 (RSM)



The following drawing illustrates the security architecture.

Host IP Assignments

IP addresses of significant hosts are listed here. In the firewall configuration, these IP addresses can be assigned these names using the `names` and `name` commands.

Host Name and Function	IP Address
vpntest, VPN test station	195.195.195.3
border, border router loopback address	195.195.195.4
nameserver; external DNS	10.1.2.35
www, customer webserver	10.1.2.36
postoffice, mailserver	10.1.2.37

Host Name and Function	IP Address
logserver, syslog server	10.1.4.40
snmpserver, network management station	10.1.4.45
authserver, RADIUS authentication	10.1.4.50
bootserver, TFTP boot/config server	10.1.4.55
sqlproxy, SQL*Net proxy server	10.1.4.58
intdns, internal DNS server	10.1.4.60

Host Name and Function	IP Address
partnerftp, partner/supplier FTP server	10.1.3.38
partnerdns, partner/supplier DNS server	10.1.3.39

Host Name and Function	IP Address
fortunedata, fortune database server	10.1.6.61

SECURITY POLICIES

In the following discussion, we refer to the networks that terminate on the firewall (other than the inside/internal network) as “service” or “perimeter” networks; the networks that terminate on the RSM (including the network that connects the RSM to the primary firewall) are considered internal networks.

Border Router Security Policy Overview

The following summarizes the security policy for the border router:

- The border router will provide ingress and egress filtering of packets with inappropriate source addresses.
- The border router will provide SYN flood protection.
- All management access to the router (including via the console) must be authenticated.

- Management access to the router via the Internet is not allowed.
- Management (access) is not allowed from any test workstations outside the firewall.
- Out-of-band access to the console port of the router will be via a passworded console server with a dial-back modem attached.
- The network management staff require access to the router (telnet) from the internal
- (GE) network.
- The router may be queried (read-only) by an SNMP-management station on the Network Services network.
- The router may initiate the following connections to the Network Services network:
  Syslog to the logging server
  TFTP to the boot/config server
  Authentication requests (RADIUS) to the authentication server.
- The router may not initiate connections to internal networks.

Ingress Filtering Details

A number of common attacks rely on spoofed source addresses. The border router provides filtering of traffic originating from the Internet (ingress filtering) to mitigate this threat.

The router is configured to deny packets with the following source addresses:

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

The router will also filter packets from the Internet claiming to have a GIAC Enterprises' address as a source:

195.195.195.0/24	GIAC Enterprises' address space (fictitious)

This list will also filter ICMP redirects; we do not want unknown parties to adjust GE's routing tables.

The access list is as follows:

```
access-list 101 deny icmp any any redirect
access-list 101 deny   ip 195.195.195.0 0.0.0.255 any
```

```
access-list 101 deny   ip 0.0.0.0 0.255.255.255 any
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
access-list 101 deny   ip 169.254.0.0 0.0.255.255 any
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any
access-list 101 deny   ip 192.0.2.0 0.0.0.255 any
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any
access-list 101 deny   ip 224.0.0.0 15.255.255.255 any
access-list 101 deny   ip 240.0.0.0 7.255.255.255 any
access-list 101 deny   ip 248.0.0.0 7.255.255.255 any
access-list 101 deny   ip 255.255.255.255 0.0.0.0 any
access-list 101 permit ip any any
```

This access list is applied to incoming traffic on the interface on the border router to the Internet:

```
ip access-group 101 in
```

Egress Filtering Details
To prevent packets with spoofed source addresses from leaving GIAC Enterprises' network, the border router will employ unicast RPF – Reverse Path Forwarding.
This is enabled on a per-interface basis and works as follows: each packet is checked as it is routed into the router. If the source IP address does not have a route in the CEF (Cisco Express Forwarding) table that points back to the same interface on which the packet arrived, the router drops the packet. The effect is to prevent spoofing attacks from originating within the GIAC Enterprises' network. This has much the same effect as an anti-spoofing egress filter, but is less CPU intensive and does not require maintenance when subnets are added to or removed from the network.

```
ip cef
interface FastEthernet0/0
    ip verify unicast reverse-path
```

Authentication for Router Management
We will set up a local user for those situations in which the internal RADIUS server is down or unreachable.

```
username netmanager password xxxxxx
```

This password will be stored as a hash, rather than clear text, in the router configuration:

```
service password-encryption
```

Use encryption for the enable password; this password will be local, rather than in RADIUS:

```
enable secret xxxxxxxx
```

Configure the console port for authentication:

```
line con 0
  exec-timeout 20 0
  login authentication console
  transport input none
  logging synchronous
```

Telnet access will only be allowed from within GE. Note that as these connections are passing through the firewall out towards the router, they will be NAT-ed.

```
access-list 19 permit 195.195.195.0 0.0.0.255

line vty 0 4
 access-class 19 in
 exec-timeout 20 0
 password 7 encrypted-localpasswd
 login
 transport input telnet
 logging synchronous
```

We will configure the router for default use of RADIUS for user-level authentication. The RADIUS server itself is configured to only accept connections from a given set of IP addresses; RADIUS also uses a pre-shared key for encryption of the password. Note that the RADIUS server will need an externally-accessible IP address so the router may query it and that incoming RADIUS requests must pass through the firewall. (Note that in the router configuration the lines won't be wrapped). 195.195.195.50 is the external IP address for this RADIUS server.

```
aaa new-model
aaa authentication login default group radius local
aaa authentication login console local
ip radius source-interface Loopback0
radius-server host 195.195.195.50 auth-port \
port#1 acct-port port#2 key pre-shared-radius-key
```

SYN Flood Protection

A SYN Flood denial-of-service attack occurs when an attacker or group of attackers flood a server or group of servers with connection requests from unreachable source addresses. The TCP intercept feature mitigates the affect of such an attack by intercepting and validating TCP connection requests.   In "watch" mode, the router software allows connection attempts to pass through the router, but the router watches to ensure that the connections become established. If the connections fail to become established within 30 seconds (configurable), the router sends a reset to the server to clear up its state. Should the number and frequency of connection attempts pass certain thresholds, the router software assumes the server is under attack and switches to a more aggressive mode, which more promptly drops connection attempts.

```
access-list 140 permit tcp 195.195.195.0 0.0.0.255
ip tcp intercept list 140
tcp intercept mode watch
```

The PIX firewall could also serve in this capacity. However, placing this function in the router removes that load from the firewall. Unfortunately, although TCP intercept activity can be monitored via the

```
show tcp intercept statistics
```

command, the router does not log what it does with regards to SYN flood attacks.

Router Self-Protection
The following configuration statements are also security-related.
Disable unneeded services:

```
no service udp-small-servers
no service tcp-small-servers
no service finger
```

Disable source routing:

```
no ip source-route

no ip finger
no ip http server

banner motd |
*** WARNING ***
[text of banner omitted]
|
```

and on the fast Ethernet interface, disable directed broadcasts so the network can't be used as a **smurf** amplifier:

```
no ip directed-broadcast
```

Other Services
SNMP: No SNMP write community string; read-only access allowed from within GIAC;

19 is the access list defining GE's external address space:

```
snmp-server community snmp-string RO 19
no snmp enable traps
```

TFTP: The router will use a set address for its TFTP requests; this can be used to lock down access to the TFTP server so that it only receives requests from valid clients.

```
ip tftp source-interface Loopback0
```

SYSLOG: The syslog server will need a static mapping between its internal, NAT-ed address and an externally-accessible address so that the router can log to it. 195.195.195.40 is the external IP address assigned to the syslog server:

```
logging 195.195.195.40 logging buffered 16000 informational
logging facility localN
logging source-interface Loopback0
```

Switch Issues

The network segment switches also use RADIUS authentication for user-level access and a local enable password. All have the HTTP service disabled and do not have an SNMP write string. The switch outside the firewall does not have an IP address assigned to it, does not use RADIUS authentication, does not have VLANs, and is only to be administered from its console port.

PRIMARY FIREWALL[1]

Primary Firewall Policy Overview

The following is a summary of the primary firewall's security policy.

DMZ Overview:

Customers (outside GE) must be able to access the company web site, with both http and SSL.
Customers must be able to send and receive e-mail to and from GE.
Customers must be able to query the external DNS server.
Mail will be proxied to the mailserver via the firewall proxy function.
Transactions between the web server and the back-end fortune database will go through a middleware proxy server.
GE employees must be able to read email from the Internet using an SSL-enabled web-mail interface.
GE employees must be able to read email from their office workstations using their regular email client.
GE employees must be able browse the company website from their workstations on the internal networks.
System and network management staff must be able to initiate access to DMZ

hosts for system management purposes.

Partner Network Overview:

See the VPN section for more details.

The DNS server on this network must be able to recursively query DNS servers on the Internet.

System and network management staff must be able to initiate access to hosts on this segment for system management purposes.

Service Network Overview:

Routers and switches (and the firewall) must be able to initiate authentication queries to the authentication server.

Routers and switches must be able to initiate TFTP sessions with the TFTP boot server.[2]

Routers, switches, and servers on all perimeter networks (including the border router) need to be able to send syslog messages to the logging server.

Hosts on internal networks need to be able to query the internal DNS server. The internal DNS server must be able to recursively query DNS servers outside of the GE network.

The SQL*Net proxy server must be able to initiate SQL*Net transactions with the fortune database server on an internal network.

The network management staff must be able to access these servers for network management purposes.

Inside Networks Overview:

All GE staff members are to have Internet access.

Hosts/users on internal networks may initiate connections to hosts on the perimeter networks.

Inbound access to these networks must be limited. The SQL*Net proxy is the only allowed inbound service.

Firewall-specific Issues:

Cisco recommends permitting ICMP unreachable messages (type 3). Denying ICMP unreachable messages disables ICMP Path MTU discovery, which can halt IPSec traffic.

The firewall will be managed from an internal network.

PIX Configuration

An initial PIX configuration is done via the console using a command line interface. For information on how to connect to the console port, see the Configuration Guide for the Cisco Secure PIX Firewall Version 6.0.

Note that some of the sample configuration lines are wrapped with a '\'; in the PIX configuration itself they would not be wrapped.

To make the configuration more readable, we enable the use of symbolic names with the

```
names
```

command, and then define names for the significant hosts listed above with commands of the form

```
name ipaddress symbolicname
```

Access for Firewall Management

The enable password (initially '**cisco**') should be re-set using the

```
enable password
```

command. We will only allow management access from the network manager subnet, 10. 1.5.0/24, and from the PIX console.

```
telnet 10.1.5.0 255.255.255.0 inside
```

The Ethernet interfaces must be brought up before **telnet** access will function.

Cisco Secure PIX Firewall Rules

The PIX uses the following features to enable and restrict access:

Interface Security Levels: Security levels allow the construction of a hierarchy of security levels among perimeter networks. This makes it simple to completely deny access from a lower-security network to a higher-security network.

NAT Statements: In addition to its roles in address-space preservation and information hiding, `nat` statements in the PIX provide simple ways to allow (or disallow, by their absence) higher-security networks to access lower-security networks.

Access Lists for Inbound Access:[3] Access lists allow connections to be initiated (generally on a restricted basis) from lower-security networks to higher-security networks. Static mappings handle the addressing issues associated with this access.

Access Lists for Outbound Access: Access lists also can deny a subset of the connections that are implicitly allowed from a higher-security to a lower-security network via a `nat` statement.

Interfaces and Security Levels

Perimeter (DMZ), inside, and outside interfaces are all assigned numerical security levels. The outside interface is always assigned 0; this indicates the lowest level of security. The inside interface is always assigned 100; this indicates the highest level of security.

Perimeter interfaces can be assigned any value in between 1 and 99, with the higher numbers indicating higher security levels. By default, hosts on higher levels can access networks on lower levels if NAT is enabled. Hosts on lower levels by default can't access higher-level (more secure) networks. Exceptions and adjustments can be configured in the firewall ruleset. If two interfaces are given the same security level, hosts on these networks will not be able to access hosts on the other network.

For this configuration we assume a single-port Ethernet card in slot 0 and a four-port Ethernet card in slot 1. The interfaces will be named and numbered as follows:

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security25
nameif ethernet3 partner security30
nameif ethernet4 service security40

ip address outside 195.195.195.2  255.255.255.0
ip address inside 10.1.1.1  255.255.255.0
ip address dmz 10.1.2.1  255.255.255.0
ip address partner 10.1.3.1  255.255.255.0
ip address service 10.1.4.1 255.255.255.0
```

Enabling Outbound Access for Inside/Internal Users
To enable access for users on the internal networks, we use the `nat` command along with the `global` command. The `nat` command permits the initiation of outbound connections; the `global` command creates a PAT address or NAT pool on a perimeter interface for use by outgoing connections.

`nat` and `global` allow for liberal outbound access; this can be tightened down in a later step with access lists.

For example, we want to enable all users on the inside networks access to the Internet. We first establish a global PAT address for use by staff members making (outbound) connections on the outside interface:

```
global (outside) 1 195.195.195.33 255.255.255.255
```

Similarly, we will create *internal* NAT pools for each perimeter interface. There is also an overflow PAT address should the addresses in the NAT pool be exhausted:

```
global (dmz) 2 10.1.2.100-10.1.2.199 \
netmask 255.255.255.0
global (dmz) 2 10.1.2.200 255.255.255.255

global (partner) 3 10.1.3.100-10.1.3.199 \
netmask 255.255.255.0
global (partner) 3 10.1.3.200 255.255.255.255


global (service) 4 10.1.4.100-10.1.4.199 \
netmask 255.255.255.0
global (service) 4 10.1.4.200 255.255.255.255
```

The number following the interface name is a NAT ID; this is used to associate `global` and `nat` statements.

For example, we want all staff members on the internal networks to be able to connect to the Internet (i.e. we want them to be able to use the global PAT address for the interface "outside"). We then associate the `global` statement with a `nat` statement for the inside interface:

```
nat (inside) 1 0 0
```

The '0 0' indicates that any host on the internal networks may initiate an outbound connection on the outside (Internet-bound) interface. If we wanted to restrict this initiation ability to a particular internal host or network, we could do so by listing the host IP or the network in place of '0 0'.

We will also let all staff (and all internal hosts) have access to all of the perimeter networks. Note the NAT IDs for each perimeter network (2=dmz, 3=partner, 4=service).

```
nat (inside) 2 0 0
nat (inside) 3 0 0
nat (inside) 4 0 0
```

Enabling Outbound Access for Perimeter Hosts
In a very similar fashion, we enable default access for higher-security networks to lower security networks.

```
nat (dmz) 1 0 0
```

On the partner network, only the DNS server has a need to access the outside network (e.g. Internet). When VPN clients are in split-tunnel mode, this will be their DNS server, and so it will need to be able to resolve queries about external hosts, including those external to GE Recall that '1' associates to the global pool for **outside**.

```
nat (partner) 1 partnerdns
```

We also enable `nat` for the service network:

```
nat (service) 1 0 0
nat (service) 2 0 0
nat (service) 3 0 0
```

Testing Access So Far

The `nat` and `global` statements do not completely implement the GE security policy for this firewall, but it would be a good idea at this point to verify that these statements as implemented function as intended. Our plan is to ping from the higher-security networks and interfaces to the lower-security networks and interfaces to verify that our access plan (as implemented so far) works. The `nat` and `global` statements will permit the outbound ICMP echo requests, but the corresponding ICMP echo replies from the lower-security networks to the higher-security networks will be denied. We need to temporarily open up access for these return ICMP packets.

- Enable the interfaces and set up default routes as described in the PIX configuration guide.
- Temporarily enable ping on all perimeter network interfaces.

The name following "access-list" and "access-group" is an access list name. Here we use a convention that visually associates it with an interface. The "any any" means from any host to any destination. The "access-group" command binds the access list to an interface. If the `nat` and `global` commands are working properly, they will let traffic exit an interface. These access lists complement the `nat/global` statements and are to let ICMP traffic enter an interface, so these are "in" or inbound access lists.

```
access-list acl_outside permit icmp any any
access-group acl_outside in interface outside

access-list acl_dmz permit icmp any any
access-group acl_dmz in interface dmz

access-list acl_partner permit icmp any any
access-group acl_partner in interface partner

access-list acl_service permit icmp any any
access-group acl_service in interface service
```

2. Turn on debugging for ICMP: `debug icmp trace`
3. Turn on syslog: `logging buffered debugging`

Before beginning the actual tests, run the following commands on the PIX to check the configuration for errors:

Command	What to Check for

`show nameif`	Verify security levels
`Show interface`	Interface and protocol are up
`show ip address`	Verify FW interfaces have correct addresses
`show global`	verify that NAT pools don't overlap; verify PAT pools don't overlap with NAT; verify IP address ranges are on the subnets for which the pool is defined.
`show nat`	Examine NAT IDs for correctness
`show route`	Verify default router to border router; static routes to networks behind the RSM.
`write terminal`	Examine configuration. Verify there are no conduit statements. Verify that there are no access lists applied with access-group commands beyond those entered for ICMP. Verify there are no other statements in the access lists beyond those entered for ICMP. Verify there is an `access-group` command for each `access-list` command.

From the PIX, ping to a host or router interface connected to each of the firewall's directly-connected network segments. This tests basic connectivity.

Now ping from the firewall to hosts or interfaces the internal segments (in this scenario we assume the RSM and Cat5k have been configured for connectivity, but no firewall rules have been installed on the RSM.). This tests routing to the internal networks.

Now from each segment directly connected to the PIX firewall, ping from a host on that segment to the corresponding firewall interface. This is a second test of basic connectivity and a test of the ICMP-permitting access lists installed above.

For the above ping tests, check the debug messages on the PIX console. Successful ping tests should result in two log entries—one for the echo request and another for the echo reply. For example, for a ping test from the border router Ethernet interface (195.195.195.1) to the outside interface on the PIX (195.195.195.2), we should see something like the following:

```
ICMP echo request (len 32 id 1 seq 256) 195.195.195.1 >
195.195.195.2

ICMP echo reply (len 32 id 1 seq 512) 195.195.195.2 >
195.195.195.1
```

All these pings should work. No debug messages at all indicate a routing or connectivity problem (or debugging is not turned on.) If a request or reply is missing its partner message, that may indicate a problem with the ICMP access lists. Refer to the PIX configuration guide for troubleshooting tips. Any connectivity, routing, and access list issues must be resolved before testing the `global/nat` statements.

Ping Through the Firewall to Test Outbound Access

To test the global/nat statements for functionality, use the following table. Use hosts or router interfaces used in the previous round of testing so we know that the router or host is able to respond to a ping.

Ping from	**To**	**Expected Result**
RSM interface 10.1.1.2 on the 10.1.1.0/ (**inside**) network	Ethernet interface, border router (**outside**)	Successful; from higher-security network
RSM interface 10.1.1.2	Host on **customer** DMZ	Successful
RSM interface 10.1.1.2	Host on **partner** network	Successful
RSM interface 10.1.1.2	Host on **service** network	Successful
Host on database server network 10.1.6.0 (**inside**)	Host on **partner** network	Successful; routing test
Host on **service** network	Ethernet interface, border router (**outside**)	Successful
Host on **service** network	Host on **customer** DMZ	Successful
Host on **service** network	Host on **partner** network	Successful
Host on **service** network	RSM interface (**inside**)	Unsuccessful; to higher security network
Proxy server (**service**)	Internal database server (**inside**)	Unsuccessful; to higher-security network
DNS server on **partner** network	Ethernet interface, border router (**outside**)	Successful; only host allowed
Other host on **partner** network (not DNS server)	Ethernet interface, border router (**outside**)	Unsuccessful; NAT not permitted.
Other host on **partner** network	Host on **customer** DMZ	Unsuccessful; NAT not permitted.
Other host on **partner** network	Host on **service** network	Unsuccessful; to higher-security network
Other host on **partner** network	RSM interface	Unsuccessful; to higher-security network
Host on customer **dmz**	Ethernet interface on border router (**outside**)	Successful

Host on customer **dmz**	Host on **partner** network	Unsuccessful; to higher-security network
Host on customer **dmz**	Host on **service** network	Unsuccessful; to higher-security network
Host on customer **dmz**	RSM interface (**inside**)	Unsuccessful; to higher-security network
VPN test client (VPN software not enabled) (**outside**)	Host on customer **dmz**	Unsuccessful; to higher-security network.

Exhaustive testing for inbound access is omitted, as there should not (yet) be anything in the configuration to allow access to internal networks or the other perimeter networks.

Enabling Inbound Access
The following table summarizes the inbound (from lower-security to higher-security networks) access needs for the perimeter networks.

Source	**Destination**	**Destination Ports**
Any external	External nameserver	53/tcp, 53/udp
Any external	Webserver	80/tcp, 443/tcp
Any external	Mail server	25/tcp, 443/tcp
Border router All dmz servers All partner servers Primary Firewall	Logging server (syslog)	514/tcp, 514/udp
Border router All dmz servers All partner servers	SNMP management station	161/udp[4]
Border router Firewall	Authentication server	1645/udp, 1646/udp
Border router Switches	TFTP boot server	69/udp
Web server	SQL*Net proxy server	1521/udp

The `nat` and `global` statements enabled outbound access (with a liberal default level of security) from higher-security networks to lower-security networks. To enable access from lower-security networks to higher-security networks, we use the `static` command and inbound access lists.

Each server on a higher-security network that will be accessed by a host or user on a lower security network needs a unique IP address assigned to it on the lower security network. That lower-security IP address is mapped to the server's real IP address with the `static` command:

```
static (high_interface, low_interface) \
     low_address high_address netmask netmask
```

The two interfaces involved are in the parentheses. The more secure interface is always listed first followed by the less-secure interface. The *high_address* is the real address of the server; the *low_address* is the address that will be used on the lower-security network in order to access the server—in essence, it's an alias.

The netmask should be 255.255.255.255 if *low_address* is a host, and a correct netmask (for *low_address*) if *low_address* is a network.

An access-list command defines how users or hosts on the lower-security network can access or use the alias address. The access list defines the IP addresses of users who can access the server/alias address, as well as what port they may use.

The general syntax is as follows:

```
access-list list-id action protocol \
     source_address port destination_address port
```

- The *list-id* is a unique name for the access list.
- The *action* is either **permit** or **deny**.
- The protocol is a valid name or number for a protocol (e.g. `tcp` or `udp`)
- The *source_address* is the host or network address for those hosts on the lower-security network that need access to the host or service on the higher-security network. If the source address is a host, it is preceded with the word **host**. If it is a network, it should be followed by a netmask.

The *destination_address* is the *low_address* (alias) defined for the server in the companion `static` statement. The host and netmask rules are the same as for the *source_address*.
Ports: Any valid port number or a valid symbolic name for a port. See the PIX configuration guide for a list of valid port numbers. The source port is rarely used and is omitted when it's not used. Precede a port name or number with the word **eq**. If all ports are to be considered or matched, omit the **eq** and port number.

An access list is bound to an interface using the `access-group` command; the list_id provides the association between the two statements as follows:

```
access-group list-id in interface low_interface
```

Inbound Access from the Internet/Outside to the Customer DMZ
Inbound access to the customer DMZ is inbound from the Internet; the low_interface is **outside**; the higher-security network customers need access to is the **dmz**, 10.1.2.0/24. The servers that need inbound access are as follows:

nameserver	10.1.2.35
www	10.1.2.36
postoffice	10.1.2.37

These each need to be associated with an address on the outside network via a `static` command.

DNS server:

```
static (dmz, outside) 195.195.195.35 10.1.2.35 \
netmask 255.255.255.255
```

Web server:

```
static (dmz, outside) 195.195.195.36 10.1.2.36 \
netmask 255.255.255.255
```

Mail server:

```
static (dmz, outside) 195.195.195.37 10.1.2.37 \
netmask 255.255.255.255
```

The above 195.195.195.*N* addresses must be listed in the external DNS as the addresses of these servers; the 195.195.195.35 (nameserver) address must be listed as authoritative for the domain **giac.com**.

Customers need to use HTTP (symbolic name www) and SSL (port 443 when encrypting HTTP) when accessing the web server.

The access list for this is as follows:

```
access-list acl_outside permit tcp any \
     host 195.195.195.36 eq www
access-list acl_outside permit tcp any \
     host 195.195.195.36 eq 443
```

This access list needs to be bound to the **outside** interface:

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

Similarly, GE staff members need SSL access to their web-based mailserver when they are outside of the office:

```
access-list acl_outside permit tcp any \
     host 195.195.195.37 eq 443[5]

access-list acl_outside permit tcp any \
     host 195.195.195.37 eq www
```

And the mailserver needs to be able to receive mail.

```
access-list acl_outside permit tcp any \
     host 195.195.195.37 eq smtp
```

Customers need access to the external DNS server:

```
access-list acl_outside permit tcp any \
     host 195.195.195.35 eq domain

access-list acl_outside permit udp any \
     host 195.195.195.35 eq domain
```

Inbound Access from the Outside to the Service Network
The border router needs access to the syslog server and the TFTP boot server. The boot and logging servers are on the network services network (10.1.4.0/24).

RADIUS server:

```
static (service, outside) 195.195.195.50 10.1.4.50 \
netmask 255.255.255.255
```

SNMP Management station:

```
static (service, outside) 195.195.195.45 10.1.4.45 \
netmask 255.255.255.255
```

Boot server:

```
static (service, outside) 195.195.195.55 10.1.4.55 \
netmask 255.255.255.255
```

Syslog server:

```
static (service, outside) 195.195.195.40 10.1.4.40 \
netmask 255.255.255.255
```

The router uses Loopback0 as its source address for syslog, tftp, and RADIUS. We assigned 195.195.195.4 to the loopback.

The ports required are

Service	**Port**
Syslog	514 udp
Syslog	514 tcp
Tftp	69 udp
Snmp	161 udp, 162 udp

Radius, radius accounting	1645 udp, 1646 udp

Syslog:

```
access-list acl_outside permit udp host 195.195.195.4 \
     host 195.195.195.40 eq syslog

access-list acl_outside permit tcp host 195.195.195.4 \
     host 195.195.195.40 eq syslog
```

TFTP:

```
access-list acl_outside permit udp host 195.195.195.4 \
     host 195.195.195.55 eq 69
```

SNMP:

```
access-list acl_outside permit udp host 195.195.195.4 \
     host 195.195.195.45 eq 161

access-list acl_outside permit udp host 195.195.195.4 \
     host 195.195.195.45 eq 162
```

RADIUS:

```
access-list acl_outside permit udp host 195.195.195.4 \
     host 195.195.195.50 eq 1645

access-list acl_outside permit udp host 195.195.195.4 \
     host 195.195.195.50 eq 1646
```

These access list statements are all additions to the same access list that's bound to the outside interface. Order doesn't matter for these list items as they are all permitting connection initiation; none of them are denying connection initiation.

Inbound Access from the Customer DMZ to the Network Service Network
The servers on the DMZ need to be able to log to the syslog server; they also need to be able to communicate with the SNMP server.

We need to set up statics (aliases) for these two servers for the DMZ; recall the DMZ is 10.1.2.0/24. For SQL*Net, we also need the following enabled on the firewall:

```
fixup protocol sqlnet[6]
```

Syslog server:

```
static (service, dmz) 10.1.2.40 10.1.4.40 \
netmask 255.255.255.255
```

SNMP station:

```
static (service, dmz) 10.1.2.45 10.1.4.45 \
netmask 255.255.255.255
```

SQL*Net Proxy Server:

```
static (service, dmz) 10.1.2.58 10.1.4.58 \
netmask 255.255.255.255
```

Note that the hosts on the DMZ will need to access or refer to these servers by their alias IPs on the 10.1.2.0/24 network rather than by their "real" IP addresses.

Syslog:

```
access-list acl_dmz permit udp 10.1.2.0 255.255.255.0 \
host 10.1.2.40 eq syslog

access-list acl_dmz permit tcp 10.1.2.0 255.255.255.0 \
host 10.1.2.40 eq syslog
```

SNMP Station:

```
access-list acl_dmz permit udp 10.1.2.0 255.255.255.0[7] \
     host 10.1.2.45 eq 161

access-list acl_dmz permit udp 10.1.2.0 255.255.255.0 \
     host 10.1.2.45 eq 162
```

SQL*Net Proxy (access from web server to proxy)

```
access-list acl_dmz permit tcp 10.1.2.36 255.255.255.0 \
     host 10.1.2.58 eq sqlnet
```

Note this is a new access list (if you have removed ICMP access); we bind it to the **dmz** interface:

```
access-group acl_dmz in interface dmz
```

Inbound Access from the Partner Network to the Network Service Network

The partner/supplier network's access needs are identical to those of the dmz with regards to the network service network.

We need to set up statics (aliases) for these two servers for the partner network; recall the partner/supplier network is 10.1.3.0/24:

Syslog server:

```
static (service, partner) 10.1.3.40 10.1.4.40 \
netmask 255.255.255.255
```

SNMP station:

```
static (service, partner) 10.1.3.45 10.1.4.45 \
netmask 255.255.255.255
```

Note that the hosts on the partner network will need to access or refer to these servers by their alias IPs on the 10.1.3.0/24 network rather than by their "real" IP addresses.

Syslog:

```
access-list acl_partner permit udp 10.1.3.0 255.255.255.0 \
host 10.1.3.40 eq syslog

access-list acl_partner permit tcp 10.1.3.0 255.255.255.0 \
host 10.1.3.40 eq syslog
```

SNMP Station:

```
access-list acl_partner permit udp 10.1.3.0 255.255.255.0 \
     host 10.1.3.45 eq 161

access-list acl_partner permit udp 10.1.3.0 255.255.255.0 \
     host 10.1.3.45 eq 162
```

Note this is a new access list (if you have removed ICMP access); we bind it to the **partner** interface:

```
access-group acl_partner in interface partner
```

Inbound Access from the Service Network to the Inside Network

The SQL*Net proxy server on the service network needs to be able to communicate with the fortune database server on an inside network.

Fortune Database:

```
static (inside,service) 10.1.4.61 10.1.6.61 \
netmask 255.255.255.255
```

SQL*Net Proxy (access from proxy to database server)

```
access-list acl_inside permit tcp 10.1.4.58 255.255.255.0 \
     host 10.1.4.61 eq sqlnet

access-group acl_inside in interface inside
```

Testing Inbound Access

Now that we have inbound access set up, we should test it before we further restrict traffic with outbound restrictions. Testing the access lists is fairly involved (see the section on Auditing the Firewall), but we can fairly easily test the static commands, and test that the access lists are bound to the interfaces with access-group commands.

Re-enable ICMP access on the firewall interfaces if you have removed it. Now repeat the ping-through-the-firewall tests. The outgoing tests that were successful should remain so.

Before testing, on the PIX, do a

```
write terminal
```

Verify that there is one access list per firewall interface (and no orphans), and that each access list has a corresponding `access-group` command.

Ping from	**To**	**Expected Result**
RSM interface 10.1.1.2 on the 10.1.1.0/ (**inside**) network	Ethernet interface, border router (**outside**)	Still successful
RSM interface 10.1.1.2	Host on **customer** DMZ	Still successful
RSM interface 10.1.1.2	Host on **partner** network	Still successful
RSM interface 10.1.1.2	Host on **service** network	Still successful
Host on database server network 10.1.6.0 (**inside**)	Host on **partner** network	Still successful; routing test
Host on **service** network	Ethernet interface, border router (**outside**)	Still successful
Host on **service** network	Host on **customer** DMZ	Still successful
Host on **service** network	Host on **partner** network	Still successful
Host on **service** network	RSM interface (**inside**)	Unsuccessful; to higher security network; no inbound access
Proxy server	Internal database server	Successful
DNS server on **partner** network	Ethernet interface, border router (**outside**)	Still successful; only this host allowed NAT
Other host on **partner** network (not DNS server)	Ethernet interface, border router (**outside**)	Still unsuccessful; NAT not permitted.
Other host on **partner** network	Customer web server (**dmz**)	Still unsuccessful; NAT not permitted.
Other host on **partner** network	RSM interface (**inside**)	Unsuccessful; to higher-security network
Host on customer **dmz**	Ethernet interface on border router (**outside**)	Still successful
External router loopback (**outside**)	195.195.195.36 (web server)	Successful
External router loopback (**outside**)	195.195.195.37 (mailserver)	Successful
External router loopback (**outside**)	195.195.195.35 (external DNS)	Successful

External router loopback (**outside**)	195.195.195.50 (RADIUS server)	Successful
External router loopback (**outside**)	195.195.195.45 (SNMP station)	Successful
External router loopback (**outside**)	195.195.195.55 (TFTP boot server)	Successful
External router loopback (**outside**)	195.195.195.40 (Syslog)	Successful
Host on customer **dmz**	10.1.2.40 (Syslog)	Successful
Host on customer **dmz**	10.1.2.45 (SNMP station)	Successful
Host on customer **dmz**	10.1.4.55 (TFTP boot)	Unsuccessful; no static
Host on **partner** network	10.1.3.40 (Syslog)	Successful
Host on **partner** network	10.1.3.45 (SNMP)	Successful
Host on **partner** network	10.1.3.55 (TFTP wannabe)	Unsuccessful; no such IP
Host on **partner** network	10.1.4.55 (TFTP)	Unsuccessful; higher sec.

Permitting Limited ICMP Traffic

When we are done testing, we need to modify ICMP access. Rather than removing it from the access lists, we will restrict it with the ICMP command. Cisco recommends that ICMP type three be permitted, as denying it entirely can halt IPSec traffic. There is an implicit deny at the end of the icmp list; ICMP types not specifically permitted are denied.

The syntax is

icmp permit|deny [**host**] *src_addr* [*src_mask*] [*type*] *int_name*

```
icmp permit 0 0 3 outside
icmp permit 0 0 3 partner
```

We also need to remove

```
debug icmp trace
```

if it is still on.

Tightening Outbound Access

With NAT enabled, outbound access is permitted by default. To fine-tune or restrict this access, we add to the access lists defined in the above sections. Our primary concern is with the perimeter networks and their hosts; these hosts have some degree of exposure to the Internet (or to each other); these hosts could conceivably be compromised. We want to reduce the possibility that a compromised host could then compromise other hosts on the network.

The following table lists the required outbound (from higher-security to lower-security) access for perimeter sources.

Source/Perimeter Host	Destination	Destination Port
Mail server	Any external	25/tcp
External DNS	Any external	53/tcp, 53/udp
SNMP Management station	dmz, partner	161/udp
Internal DNS	Any external	53/tcp, 53/udp
Partner DNS	Any external	53/tcp, 53/udp

Restricting Outbound Access from the DMZ Network
Only the mail server and DNS server need to initiate outgoing requests:

Mail Server:

```
access-list acl_dmz permit tcp \
     host 10.1.2.37 any eq smtp
```

DNS:

```
access-list acl_dmz permit tcp \
     host 10.1.2.35 any eq domain

access-list acl_dmz permit udp \
     host 10.1.2.35 any eq domain
```

Deny initiating other outbound connections to the outside interface:

```
access-list acl_dmz deny ip 10.1.2.0 \
     255.255.255.0 any
```

The order matters for these statements; the permit statements need to appear before the deny statement. In general, more specific statements should appear before more general statements. In this situation (and for all our current rule sets) the permit is more specific than the deny statement, and so the permit should appear before the deny statement. For our current rule set, our deny statements should appear at the end of our access lists for all our lists. Connections not explicitly matched by the access list are handled in the following fashion:

- An explicit permit for connections to a lower-security network allowed via a nat statement.
- An explicit deny for connections to a higher-security network.

Restricting Outbound Access from the Partner Network
The partner network is already fairly restricted, as only the DNS server is allowed to initiate outbound connections. We can further restrict the DNS server's activity to just DNS.

```
access-list acl_partner permit tcp \
     host 10.1.3.39 any eq domain

access-list acl_partner permit udp \
     host 10.1.3.39 any eq domain
```

Deny other access to other networks:

```
access-list acl_partner deny ip 10.1.3.0 255.255.255.0 \
     any
```

Restricting Outbound Access from the Services Network

Similarly, we restrict outbound access from the services network:

SNMP server, to border router:

```
access-list acl_service permit udp \
     host 10.1.4.45 host 195.195.195.4 eq 161
```

SNMP server, to dmz:

```
access-list acl_service permit udp \
     host 10.1.4.45 10.1.2.0 255.255.255.0 eq 161
```

SNMP server, to partner:

```
access-list acl_service permit udp \
     host 10.1.4.45 eq 10.1.3.0 255.255.255.0 eq 161
```

DNS:

```
access-list acl_service permit tcp \
     host 10.1.4.60 any eq domain

access-list acl_service permit udp \
     host 10.1.4.60 any eq domain
```

Deny other access:

```
access-list acl_service deny ip 10.1.4.0 255.255.255.0 \
     any
```

Syslog for the Firewall

Once initial testing is complete, the firewall should be configured to log to a syslog server:

```
logging host service logserver
```

`service` is the network service network; `logserver` is the symbolic name for the syslog server on that network.

logging level should be changed to a level lower (less detailed) than **debugging**. The `logging trap` command sets the level for syslog messages:

```
logging trap notifications
```
[8]

Set the clock with the `clock set` command, and then enable timestamps for the syslog entries:

```
logging timestamp
```

Mail Proxy
The command

```
fixup protocol smtp
```

enables the MailGuard feature, which only lets mail servers receive the RFC 821, sec. 4.5.1 commands:

HELO
MAIL
RCPT
DATA
RSET
NOOP
QUIT

All other commands are rejected.

Protection for Authentication Servers
The command

```
floodguard 1
```

provides some denial-of-service-attack protection for an authentication server. It controls the AAA service's tolerance for unanswered login attempts. Floodguard is enabled by default. As the authentication server is accessible from the Internet, a denial-of-service attack is a possibility.

VPN Access
Partners and suppliers will use VPN clients for secure access to upload and download fortune files. The partners will be supplied with Cisco's VPN 3000 client, version 3.0. This client version supports Windows 95, Windows 98, Windows ME, NT 4.0, and Windows 2000. Customer Care will provide technical support for suppliers and partners. Customer Care has asked that a test Windows platform be connected (using a switch) *outside* the primary firewall so that Customer Care can test VPN connectivity as well as test SOHO firewalls and personal firewall software for compatibility with the VPN client

software. Customer Care plans to be able to recommend compatible combinations to suppliers and partners and to assist with configuration issues. Customer Care has agreed to keep the workstation up-to-date with regards to patches and virus software, to not move the test workstation back behind the primary firewall and to leave the workstation turned off when not in use.

VPN Policy Overview
The following briefly describes the security policy for VPN access.

- VPN tunnels terminate on the primary PIX firewall.
- Each VPN user has a unique username with an associated password.
- A VPN user's username and password will be revoked if/when his association with GE ends.
- Partners and suppliers will use the same authentication server as used by internal staff. (Note that the RADIUS client is the firewall; not the partner/supplier PC.) However, partners and suppliers will be placed in a separate RADIUS realm (a separate namespace) so that partner usernames can be easily differentiated from staff usernames.
- Authentications and authentication attempts will be logged.[9]
- VPN clients are allowed normal customer-level access.
- In addition to customer-level access, VPN clients have access to the necessary servers on the partner/supplier network, but will not have access to other GE internal networks.
- VPN clients will be provided with (very limited) internal DNS for the partner/supplier network, but will not have access to internal DNS for the rest of the company.
- Each VPN partner company or supplier company or organization will have a unique key.
- Keys will be removed for partners or suppliers whose relationship with GE ends.
- Keys will be pre-shared.
- VPN clients will use split tunneling; the split tunnel will allow the VPN clients access to the required servers inside GE, while still allowing non-encrypted traffic to Internet-accessible servers.
- The VPN tunnel will be defined restrictively via split-tunneling; i.e. not all internal hosts or internal networks will be accessible via the VPN tunnel. Traffic to these protected internal hosts will not be included in the tunnel; these host addresses are non-routable, and so the connection attempt will fail.
- VPNs will use both an ESP encryption transformation for data confidentiality and an AH transform for data authentication for the outer IP header as well as the payload data.

VPN Configuration Details for the Primary PIX Firewall

Transform Selection

The PIX provides to ESP transforms: esp-des and esp-3des. Cisco suggests the following transform combinations:

ESP Transform	AH Transform
esp-3des	esp-sha-hmac
esp-des	esp-sha-hmac

GE will use DES to accommodate partners and suppliers who may not be able to use 3DES.

The following is an annotated description of the PIX configuration statements used to configure VPNs on the PIX in accordance with the security policy outlined above. Note that in the PIX configuration the lines will not be wrapped; they are wrapped here with a '\' for readability.[10]

10.1.8.0/24 will be used as the address pool for the partners and suppliers. We set up an IP address pool for VPN clients:

```
ip local pool partnerpool 10.1.8.1-10.1.8.254
```

Packets with their source on the partner network with a VPN client as a destination must not undergo NAT. The following access list identifies those outbound packets. Note that 10.1.3.0/24 is the partner/supplier network.

```
access-list 101 permit ip 10.1.3.0 255.255.255.0 \
10.1.8.0 255.255.255.0
```

Now we bind ACL 101 to the NAT statement to avoid NAT on the IPSec packets. '`nat 0`' is the 'disable NAT' command.

```
nat (partner) 0 access-list 101
```

Define a RADIUS server; RADIUS will be its name.

```
aaa-server RADIUS protocol radius
```

The clear-text pre-shared key is for password encryption between the RADIUS server and RADIUS client.

```
aaa-server RADIUS (service) \
host authserver shared-key timeout 5
```

The `sysopt` command implicitly allows/trusts IPSec encrypted traffic. IPSec traffic will bypass conduit, outbound list, and interface access list blocking.

```
sysopt connection permit-ipsec
```

Select DES for the ESP payload encryption and esp-sha-hmac for the AH transform. A transform set is a combination of security protocols and algorithms. During negotiation the peers agree to use a particular transform set. 'reg-des' is the name of the transform set.

```
crypto ipsec transform-set reg-des esp-des esp-sha-hmac
```

Crypto maps specify IPSec policy. Maps group together details such as transform sets addresses, and how security assoc. are to be established. Only one crypto map set can be applied to any given interface. The '10' here is a sequence numbers. For situations in which there are multiple entries, the sequence number indicates which entry is preferred or higher priority. This is a dynamic crypto map; dynamic maps are used for VPN peers.

```
crypto dynamic-map dynmap 10 set transform-set reg-des
```

Add the dynamic map to the (static) map set. In this case, as there aren't any non-VPN-client peers, and therefore no static entries; the dynamic entry is the only entry in the map set. The '10' is a sequence number; if there were static entries, we would give the dynamic entry a high sequence number so that static entries would be examined first.

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

Allow the firewall to download an IP address to peer as part of the IKE configuration:

```
crypto map partner-map client configuration address \
initiate
crypto map partner-map client configuration address respond
```

Require authentication; tie the map to the AAA server defined above.

```
crypto map partner-map client authentication RADIUS
```

The following statement binds the IPSec engine on the outside interface. Note that 'outside' is the name assigned to the outside interface.

```
crypto map partner-map interface outside
```

ISAKMP is an Internet Security Association and Key Management Protocol; this is a protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol and the negotiation of a security association.[11]

The following statement enables ISAKMP so security associations can be negotiated between clients and the outside interface.

```
isakmp enable outside
```

VPN Clients will specify the outside address of the PIX as their peer.

```
isakmp identity address
```

The following is an ISAKMP Policy for 3000 VPN client running 3.0 code. ‘10’ is a priority, should more than one policy set be specified.

```
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
```

‘Group 2’ is Diffie-Hellman group 2 and is required for the client version we are using.

```
isakmp policy 10 group 2
```

The SA will last one day (i.e. have a lifetime of one day)
before expiring.

The following are access list defining those hosts that partners/suppliers may access. Traffic to these two servers is included in the VPN tunnel. Traffic to other destinations is unencrypted and not included in the tunnel.

DNS server
```
access-list 125 permit ip host partnerdns \
10.1.8.0 255.255.255.0
```
FTP server
```
access-list 125 permit ip host partnerftp \
10.1.8.0 255.255.255.0
```

IPSec group configuration follows. We define one group per supplier or partner company; only one group is shown here. A different group would have a different name and a different key. Multiple groups may share the same IP address pool. Keys are associated with VPN group IDs rather than IP addresses, so IP addresses may be assigned dynamically. Note the split tunnel destinations are bound to the VPN client here.

```
vpngroup supplier1 address-pool partnerpool
```

Partner network DNS server
```
vpngroup supplier1 dns-server partnerdns
vpngroup supplier1 default-domain giac.com
vpngroup supplier1 split-tunnel 125
vpngroup supplier1 idle-time 1800
vpngroup supplier1 password supplier1-pre-shared-key
```

VPN Client Configuration
VPN client configuration is fairly simple.

- Launch the 3000 VPN client.[12]
- Click **New** to create a new connection
- Enter *GIAC* (or another name) under **Connection Entry**
- Enter the outside address of the primary firewall under **Host name or IP address**: *195.195.195.2* or *vpn-server.giac.com*
- Under **Group Access Information**, enter the VPN group name (e.g. *supplier1*) and the corresponding group password (i.e. the pre-shared key).
- Click **Next**.
- Click **Finish**.

Using the VPN Client
Launch the 3000 VPN client.
Select the GIAC connection from the drop-down list.
Click **Connect**.
The window shows: "Negotiating security profiles"
When the **xauth** (extended authentication) window appears, enter your individual (RADIUS) username and password.

Testing the VPN
Customer Care has requested a VPN test client be made available for its use; it can be used for the following tests of VPN functionality and of the security expected to be provided via the firewall and the split tunnel restriction.

Test	**Expected Result**
Authenticate via RADIUS	Successful
FTP to ftpserver	Successful
http access to www.giac.com	Successful
ping backupserver on partner network	Unsuccessful
Ping firewall interface on partner network	Unsuccessful

The first time we attempt an authentication with the RADIUS server via the firewall client, we should check the RADIUS log to see which interface the PIX uses as its source. That interface must be added to the list of allowed clients for the RADIUS server.

AUDIT

Audit Procedures for the Primary Firewall

Auditing an element of the security architecture can accomplish or assist with the following:

- If this is the first audit performed, the audit establishes a baseline against which future audit results can be compared.

- For subsequent audits, an audit can determine what has changed with regards to the security implementation.

- An audit can demonstrate that a device is not configured or operating in accordance with security policy.

- An audit can indicate problems, overlooked issues, and areas for improvement.

The audit procedure described here focuses on first three bullet items. This procedure will produce a baseline of results for comparison with the security policy and for comparison with subsequent audits. It does not directly assess the quality of the security policy, and so (except in those situations where errors are located) and therefore does not necessarily point out areas for improvement.

Audit Considerations

Although audit tools and procedures may be developed by outside consultants, the GE networking staff should be part of the audit process and at the very least be trained in using the audit tools and techniques. Networks, systems, and security devices are not static. Networks should and do change to meet changing business needs. The GE staff needs the tools, techniques and training at their disposal to verify that security is still sound.

The audit itself should be performed during GE's maintenance window. The full audit procedure requires taking network segments and critical hosts offline, and therefore will disrupt connectivity for both customers and staff.

Audits can be time-consuming. For an audit of the primary firewall, consider the following as rough estimates:

- Checking security advisories: one hour
- Deciding what to scan; preparing shell scripts or batch files: 30 minutes per interface
- Scanning per interface: two hours
- Analysis of results: Two hours and up

Audit Tools

For this audit, we use a free scanner, **nmap**, from http://www.insecure.org/nmap. An NT version is available if the audit staff prefers NT over Unix. We will be using **nmap** primarily as a traffic generator. **nmap** should be installed on a laptop computer for mobility. We also require at least one sniffer; one sniffer per network interface (for a total of five) would greatly speed the process. The ping tests require at least two laptops. Our other audit tool is the firewall itself.

Audit Costs

Assuming the staff already has the required equipment, the audit costs can be roughly estimated by figuring the labor costs. Not included in the rough estimate, though, is the time it can take to troubleshoot unexpected results and resolve related issues, which may ultimately be the most important phase of the audit.

Audit Procedures

Review Security Advisories

GE's security policies and procedures include procedures for keeping the firewall up-to-date with regards to known vulnerabilities. This step in the audit is a check on that process. For the PIX firewall, we check and record its current version with the command

```
show ver
```

record the current version. Now we check online security advisories for known bugs or vulnerabilities. For Cisco equipment, these are available at the following URL:

http://www.cisco.com/warp/public/707/notices.html

This lists both of Cisco's security advisories and security advisories at

http://www.securityfocus.com

If search this reveals a vulnerability that needs to be addressed, the audit team may want to correct the problem prior to proceeding with the audit. Alternatively, the audit team could conduct a the portion of the audit that should or might detect the vulnerability, then correct the problem, and repeat that portion of the audit.

Ping Tests

The purpose of the following set of ping tests is to verify that the interface security levels are still in place, and that NAT between the perimeter networks is still working as expected.

In preparation for this test, we un-restrict ICMP. We also verify that the ICMP permits we placed in the interface access lists during initial testing are still in place.

```
clear icmp
```

Make a note to restore the settings after testing. The ICMP permit statements must be in the access lists bound to each interface and that the permit statements for ICMP appear before any deny statements that would block them. Verify this with

```
show access-list
```

The endpoints of our ping tests need to be host IP addresses that are not in use on our networks and that are not listed in the firewall rule sets. The test laptops can be used as source and destination machines.

Before proceeding with the test, verify that the test laptops can send and receive pings by pinging the nearest firewall interface.

In this table, is an unused host IP on the perimeter network under test; D is an unused host IP on the destination perimeter network.

Source	Destination	Expected Result
10.1.2.S	195.195.195.1	Successful
10.1.2.S	10.1.3.D	Unsuccessful
10.1.2.S	10.1.4.D	Unsuccessful
10.1.2.S	10.1.1.D	Unsuccessful
10.1.3.S	195.195.195.1	Unsuccessful; restricted NAT
10.1.3.S	10.1.2.D	Unsuccessful; restricted NAT
10.1.3.S	10.1.4.D	Unsuccessful
10.1.3.S	10.1.1.D	Unsuccessful
10.1.4.S	195.195.195.1	Successful
10.1.4.S	10.1.2.D	Successful
10.1.4.S	10.1.3.D	Successful
10.1.4.S	10.1.1.D	Unsuccessful
10.1.1.S	195.195.195.1	Successful
10.1.1.S	10.1.2.D	Successful
10.1.1.S	10.1.3.D	Successful
10.1.1.S	10.1.4.D	Successful

“Unsuccessful” indicates there is not wide-open inbound network access between the networks.

Scanning/Traffic Generation

This portion of audit includes scanning of the firewall to determine what is enabled by the rule sets; we will then compare what the rule sets permit with what is allowed by the security policy. We will also check what traffic is actually permitted by the firewall, in order to verify that the firewall permits what is specified in the rule sets and nothing else; this is a check on the firewall's veracity. This step requires a quiet network, as we will be dealing with NAT-ed traffic. We ultimately want to be able to tell what access is permitted through the firewall.

Towards this end, we will first locate static mappings. Recall that static mappings are to allow access from a lower-security network to a higher-security network.

- The interface is a lower-security interface. We will call this network **outside**.
- There exists a host on a higher-security network. We will call this higher-security network **inside**.
- There is a static mapping that associates an address on the **outside** network with the host's real address on the **inside** network. We will call this alias address on the **outside** (lower security) network **outside-alias**.

We are looking for these **outside-aliases** on the lower-security networks.

For example, the syslog server is on a higher-security network (**service**) than the hosts on the DMZ network, and yet the hosts on the **dmz** need to be able to access the syslog server.

Detecting Static Mappings with a Ping Scan
For this test, we still need ICMP enabled as above.

Enable viewing of trace and log messages at the console or in your terminal session on the PIX with

```
terminal monitor
```

now enable ICMP trace:

```
debug icmp trace
```

Capture the terminal output with your terminal program; it is this output we will use for the audit, and the ICMP traces do not go to syslog.

For each interface, from a host on that network, ping the entire address range for that network with **nmap**. In this example we show pinging the DMZ hosts:

```
nmap  –v  –sP  10.1.2.0/24
```

For each static mapping of a higher-security host to this segment, in the PIX log you will see a trace message like the following:

```
63: Inbound  ICMP echo request (len 56 id 40555 seq 13)
10.1.2.nmaphost >.10.1.2.40 > 10.1.4.40
```

The NAT address on the **dmz** for the syslog server is 10.1.2.40; its real IP address on the **service** network is 10.1.4.40.

nmap will report the host as down if the host does not reply to the ping; the ICMP trace is the more reliable indicator of the existence of the static mapping.

Which ports are permitted for which hosts?
The existence of a static mapping does not necessarily mean a host is reachable (other than by our temporarily-enabled ping test); that host's NAT address (from the static mapping) has to appear in an inbound access list that's bound to the interface for this network.

Which ports do we have to scan?
The quick answer would be "all of them". However, scanning can be time consuming and we want this audit to finish in a finite amount of time. With a little work, we can narrow down the list. We do a

```
show access-list
```

Make a note of ports listed after the **eq** in the access lists. Make a note of any destination hosts that don't have **eq** and a port number listed. We will add the telnet and ftp ports to our scan, since these would be common ones to be opened up "temporarily." If the audit staff is aware of other ports that have been troublesome or suspect in the past, the team can add those ports to the audit.

Again we will be watching the PIX log for information. Make sure that the PIX is writing to a syslog server; we will be using syslog information for the audit.

Where do we scan from?
We will use **nmap** to spoof scans from the addresses of the servers that are on the perimeter network we are examining. Again, this is a compromise to save time; the more exhaustive technique would be to spoof scans from all the addresses in the address space. While we spoof a server's address, the server should be taken offline. For those tests involving a source or destination perimeter network, we will take the outside and inside networks down so as to eliminate spurious traffic. If taking the network segments offline is not possible, the audit team can omit the use of the sniffer on the destination network and rely on just the firewall log. This places greater trust in the firewall as there is no check that the firewall is actually doing what the rule set says.

For our current configuration, for the **outside** network, we end up with the following information:

Target NAT Addresses	Ports	Source addresses
195.195.195.35 ext-dns 195.195.195.36 web 195.195.195.37 mailserver 195.195.195.40 syslog 195.195.195.45 snmp 195.195.195.50 auth 195.195.195.55 boot	For Internet-accessible servers, we should do a complete scan of both TCP and UDP ports.	Any unused address outside the firewall; border router

For the **dmz** network, we end up with the following:

Target NAT Addresses	Ports	Source addresses
10.1.2.40 syslog 10.1.2.45 snmp 10.1.2.58 sqlnet	80/tcp, 443/tcp, 25/tcp, 53/udp, 53/tcp, 514/tcp, 514/udp, 69/udp, 161/udp, 162/udp, 1645/udp, 23/tcp, 21/tcp, 1645/udp, 1521/tcp	nameserver www postoffice backupserver

For the **partner** network, we end up with the following:

Target NAT Addresses	Ports	Source addresses
10.1.3.40 syslog 10.1.3.45 snmp	80/tcp, 443/tcp, 25/tcp, 53/udp, 53/tcp, 514/tcp, 23/tcp, 21/tcp, 514/udp, 69/udp, 161/udp, 162/udp, 1645/udp, 1646/udp, 1521/tcp	partnerftp partnerdns backupserver

For the **service** network, we end up with the following:

Target NAT Addresses	Ports	Source addresses
10.1.4.61 fortunedata	80/tcp, 443/tcp, 25/tcp, 53/udp, 53/tcp, 514/tcp, 514/udp, 69/udp, 161/udp, 162/udp, 1645/udp, 1646/udp, 1521/tcp, 23/tcp, 21/tcp	logserver, snmpserver, authserver, bootserver, sqlproxy, intdns

Note that the content of the above tables will differ from what you see here if the firewall configuration has changed.

From the above tables, we construct a series of scans to be conducted from (and on) the four perimeter networks. The **nmap** flags we will need are as follows:

Flag	Meaning
-P0	(zero) don't ping
-sU	UDP scan, for the udp ports
-sT	TCP scan, for the tcp ports
-v -v	very verbose
-o logfilename	Normal logfile; for resuming interrupted scans
-p *n1,n1,n3,n4*	Listed port numbers to scan
-S *spoofed-source*	Spoof the source address
-e *ethernetinterface*	Interface on the **nmap** laptop

For example, to scan the syslog server from the **dmz** network:

```
nmap -v -v -P0 -sU -p 53,514,69,161,162,1645,1645 \
     -S 10.1.2.35 -e hme0 10.1.2.40
```

We put a sniffer on a spanning port on the switch on the destination network (i.e. the network where the NAT'ed target host actually resides.) The sniffer will provide us with a record of the actual traffic that passes through the firewall.

After we've completed a scan from a given (spoofed) source address, we'll retrieve our results from the syslog server, record our sniffer results, and then put the server back on line.

If a port is permitted by the firewall, you will see a "Built" entry like the one below.

```
302005: Built UDP connection for faddr 10.1.2.35/37847 gaddr
10.1.2.40/514 laddr 10.1.4.40/514
```

`faddr` is the "from address", i.e. the source address.
`gaddr` is the "global address", i.e. the NAT address.
`laddr` is the "local address", i.e. the real address.
The successful port in this example is UDP syslog.
Unsuccessful probes resemble the following:

```
106019: IP packet from 10.1.2.35 to 10.1.2.40, protocol udp
received from interface "dmz" deny by access-group "acl_dmz
"
```

Expected Scan Results
From the PIX-generated syslog entries, you can build a table of successful connections between source addresses and destination addresses/ports.

The following are the expected successful results:

Target (Real)	Dest Port(s)	Source Hosts
nameserver, ext-dns	53/tcp, 53/udp	Any external
web	80/tcp, 443/tcp	Any external
postoffice, mailserver	25/tcp, 443/tcp	Any external
logserver,syslog	514/udp, 514/tcp	Border router, any perimeter host, any internal host
snmpserver	161/udp, 162/udp	Border router, any perimeter or internal host
authserver	1645/udp, 1646/udp	Border router
bootserver	69/udp	Border router
sqlproxy	1521/tcp	web
intdns	53/tcp, 53/udp	internal host
fortunedata	1521/tcp	sqlproxy

VPN Testing

The audit team should repeat the VPN functionality testing steps listed in an earlier section.

Audit Evaluation

First-phase audit evaluation tasks include the following:

- Compare current audit results to security policy
- Compare current audit results to baseline audit results
- Compare the firewall log results to the sniffer log results

For detected differences, the audit team needs to determine the cause of the difference, and take an appropriate action. Possible actions could include the following:

- Correct a configuration error and re-run the portion of the audit that detected the error.
- Evaluate the implications of a change in the firewall ruleset; perhaps modify the change/difference.
- Add a change to the baseline.
- Suggest modifications to the security policy to make it more in line with business needs.
- Suggest modifications to business practices to make them more in line with security needs.
- Re-visit change management procedures to improve the way changes are implemented and documented.

Potential Areas for Improvement

Outbound access from the inside networks is quite liberal. This could be restricted, provided the networking staff is provided with detailed information on the types of access that staff members need and expect. As far as is reasonable, security should not interfere with business functions. On other fronts, should GE become a 24/7 business, GE may want to add some redundancy to the network. GE may want to add a second firewall for failover purposes. This simplifies upgrades, as the not-in-use firewall can be upgraded first. GE could also add some redundant servers—secondary DNS and authentication servers would add to reliability and ease upgrades. A second Internet connection may also assist with reliability.

DESIGN UNDER FIRE

For the penetration analysis of a very different architecture, I have selected Gale Slentz' firewall practical. The paper is available at http://www.sans.org/giactc/gcfw.htm. A drawing illustrating the architecture from the paper is included as an appendix.

Attack Against the Firewall

The primary firewall in this architecture is CheckPoint Firewall-1, Version 4.x, running under Solaris 8. The version is unspecified, but a web search reveals that 4.1 runs on Solaris 8[13], although Checkpoint does not provide technical support for all 4.1*n* versions under Solaris 8. So we can fairly safely assume the firewall is some unspecified release of 4.1.

Checking the Bugtraq database at http://www.securityfocus.com, we find the following vulnerabilities for 4.1:

Bugtraq ID	Date	Notes	This design vulnerable?
3300	2001-09-08	Policy name file vulnerability	No; requires local user.
3058	2001-07-18	SecureRemote Info leak	Information gathering; not an attack
3021	2001-07-11	VPN user can gain control of mgt. station	No; must be authenticated VPN user.
1534	200-08-02	TCP access to any port on protected destination, providing RSH/REXEC enabled for that host with STDERR port.	Not unless administrator "temporarily" enables rsh w/stderr and then forgets.

1662	2000-08015	Session agent password guessing	Not using session agent.
1312	2000-06-06	Illegally frag. packets cause DoS	YES, if version is 4.1
1419	2000-07-05	Spoofed UDP pkts cause crash; vendor can't reproduce.	Vulnerability may not exist.
2238	2001-07-11	Source routed pkts cause DoS	No, providing router has no ip source rt. as is specified in policy.
3336	2001-09-12	Buffer overflow root exploit. Must be permitted to view logs with GUI.	No; no remote management of firewall.

For #ID 1312, a demonstration exploit is posted. If the firewall version is plain 4.1, the attack may succeed in causing a denial-of-service. The simple remedy is to upgrade the firewall to 4.1*n*.

Denial-of-Service Attack

For devising a denial-of-service attack against this network, we're to assume we (the attackers) have control of fifty compromised cable modem connections. We can fairly safely assume that among those fifty cable-modem users we have some Linux boxes. We will install **papasmurf-linux**, available from http://packetstormsecurity.org/, on the Linux boxes.

For a **smurf** attack, we need to use amplifier networks. We can locate them with **nmap**:[14]

```
nmap -n -sP -PI -o smurf.log \
 'XXX.YYY.*.0,63,64,127,128,191,192,255'
```

In the above example, we are looking for six-bit subnets in a class B address space *XXX.YYY*.0.0/16.

Counter Measures

The firewall in this design is configured to drop ICMP packets and will do so. The real issue (assuming a high enough ICMP flood level) will be saturation of the bandwidth from the local ISP to GE. Cisco has devised a handy input access list for a router that is useful for diagnosing the type of attack; its use is described in the white paper "Characterizing and Tracing packet floods using Cisco Routers."[15] This will allow the networking staff to determine what kind of flood attack they are experiencing so they may take appropriate measures. The best option for a site experiencing a **smurf** attack is to contact the upstream to have the traffic blocked or limited.

.

Internal System Compromise

Our third attack attempt will be against a system behind the firewall. The external DNS server resides on the service network. The design does not specify its operating system version, but as the web server and firewall are Solaris 8, the DNS server might also be Solaris 8, and it might be running the version of BIND distributed by Sun. Sun recently (6/26/01) released BIND patches for Solaris 8; these are to patch a re-introduced buffer overflow vulnerability with TSIG, the transaction signal handling code. The practical specifically mentions a stack-based-buffer-overflow hardening step for the web server, but does not mention it for the DNS server. **Bind8x**[16], available from Packetstorm, is allegedly an exploit program for this vulnerability.

However, due to restrictive firewall rules, the attacker still has a problem. Once he has compromised the server, he needs to be able to connect to the DNS server in some way to manipulate it, and if he collects data locally, he needs a way to send home the data he collects. Restrictive firewall rules greatly limit his options, barring firewall configuration errors. He could, however, cause a temporary denial-of-service attack by corrupting some critical file or files on the DNS server via the exploit. There is not a second external DNS mentioned in the design; if this DNS server is down, customers can not reach the GE website or mail server.

References

Cisco Systems, Security advisories and notices
http://www.cisco.com/warp/public/707/notices.html

Cisco Systems, *Cisco Secure PIX Configuration Guide, 6.0*
URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/config

Cisco Systems, *IPSec User Guide for the Cisco Secure PIX, 6.0*
URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/ipsec/

Cisco Systems, "How to Add AAA Authentication (Xauth) to PIX IPSec 5.2 – 6.0"
URL:
http://www.cisco.com/warp/public/110/pixcryaaa52.shtml

Cisco Systems, "Configuring Cisco Secure PIX Firewall 6.0 and Cisco VPN 3000 Clients Using IPSec"
URL:
http://www.cisco.com/warp/public/110/pix3000.html

Cisco Systems, "Characterizing and Tracing packet floods using Cisco Routers"
http://www.cisco.com/warp/public/707/22.html

Huegen, Craig, "The Latest in Denial of Service Attacks: "Smurfing"; Description and

Information to Minimize Effects", Feb., 2000
URL: http://www.pentics.net/denial-of-service/white-papers/smurf.txt

Finding smurf amplifiers:
URL: http://packetstormsecurity.org/9901-exploits/smurf.BIP-hunting-nmap.txt

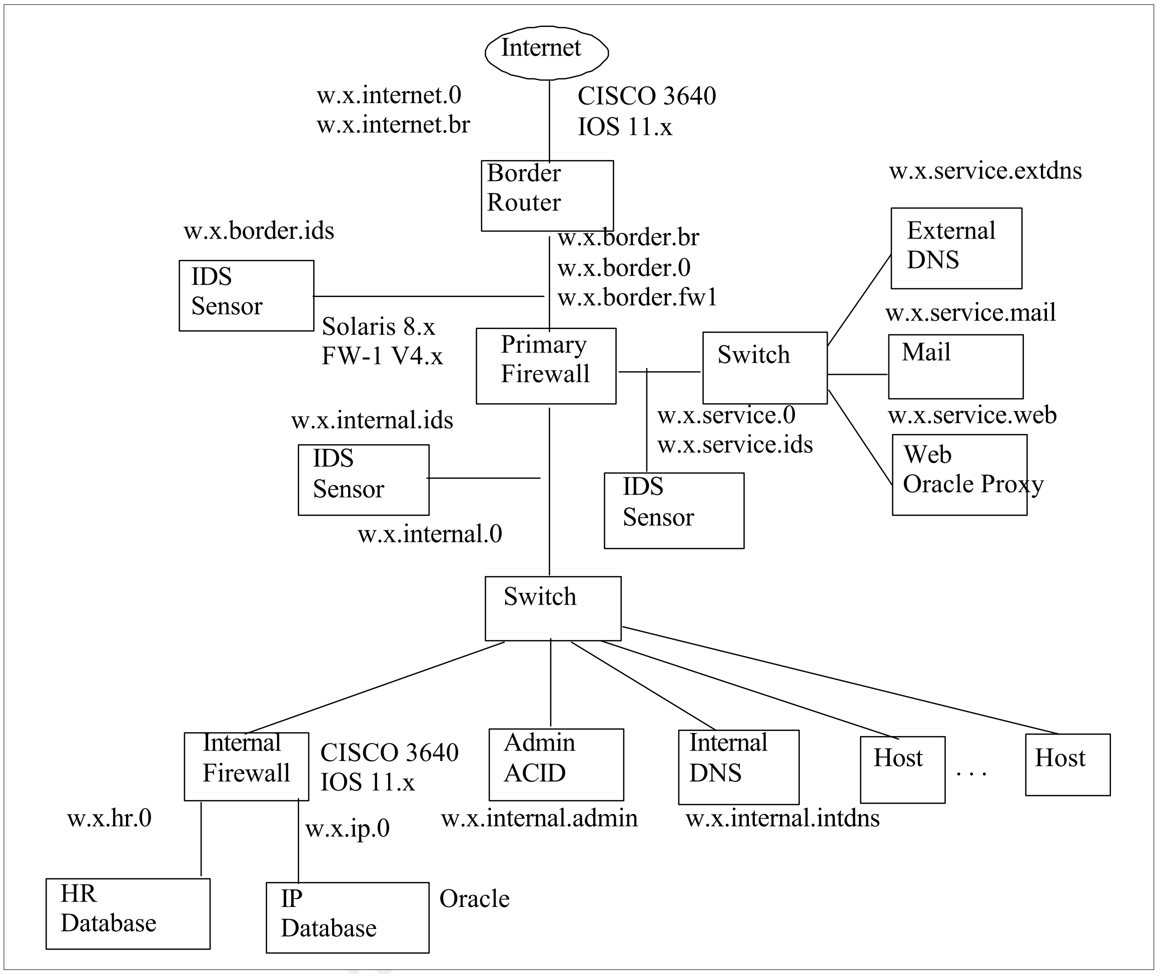
Sun Microsystems, Bulletin #002204 (BIND), June 26, 2001:
http://archives.neohapsis.com/archives/sun/2001-q2/0002.html

CERT, BIND Vulnerabilities:
http://www.cert.org/advisories/CA-2001-02.html

nmap: http://www.insecure.org/nmap/

Exploit code archive:
http://packetstormsecurity.org/

APPENDIX: Design Under Fire Architecture, Gale Slentz



END NOTES

[1] This section covers both a description of the security policy and a tutorial on how to implement it.

[2] The PIX firewall won't be able to use this TFTP boot/configuration server. A PIX's TFTP server must be on its inside network. However, if the TFTP server were on the inside network and the border router were to use it, the border router would have to be able to make a direct connection to the inside network. The best workaround is two TFTP boot servers.

[3] The older conduit statement also serves this function.

[4] We are using polling for all monitored stations, plus traps for the border router.

[5] If the web-based mail server encrypts POP with SSL, the firewall will need to admit port 995; if it encrypts IMAP with SSL, the firewall will need to admit port 993.

[6] Cisco assumes SQL*Net version 1, TCP 1521. SQL*Net version 2 is 1525. Cisco says the following about the fixup command: "The [SQL*Net] protocol consists of different packet types that PIX Firewall handles to make the data stream appear consistent to the Oracle applications on either side of the firewall."

[7] PIX uses a netmask, rather than the wildcard that Cisco IOS uses.

[8] Cisco recommends setting the level to **errors**, which is two levels lower than **notifications**.

[9] Merit RADIUS (now InterLink Networks RADIUS) logs locally to the RADIUS server; other versions may use syslog.

[10] VPN configuration adapted from http://www.cisco.com/warp/public/110/pix3000.html

[11] IPSec User Guide for the Cisco Secure PIX Firewall Version 5.3 pg. 1-2.

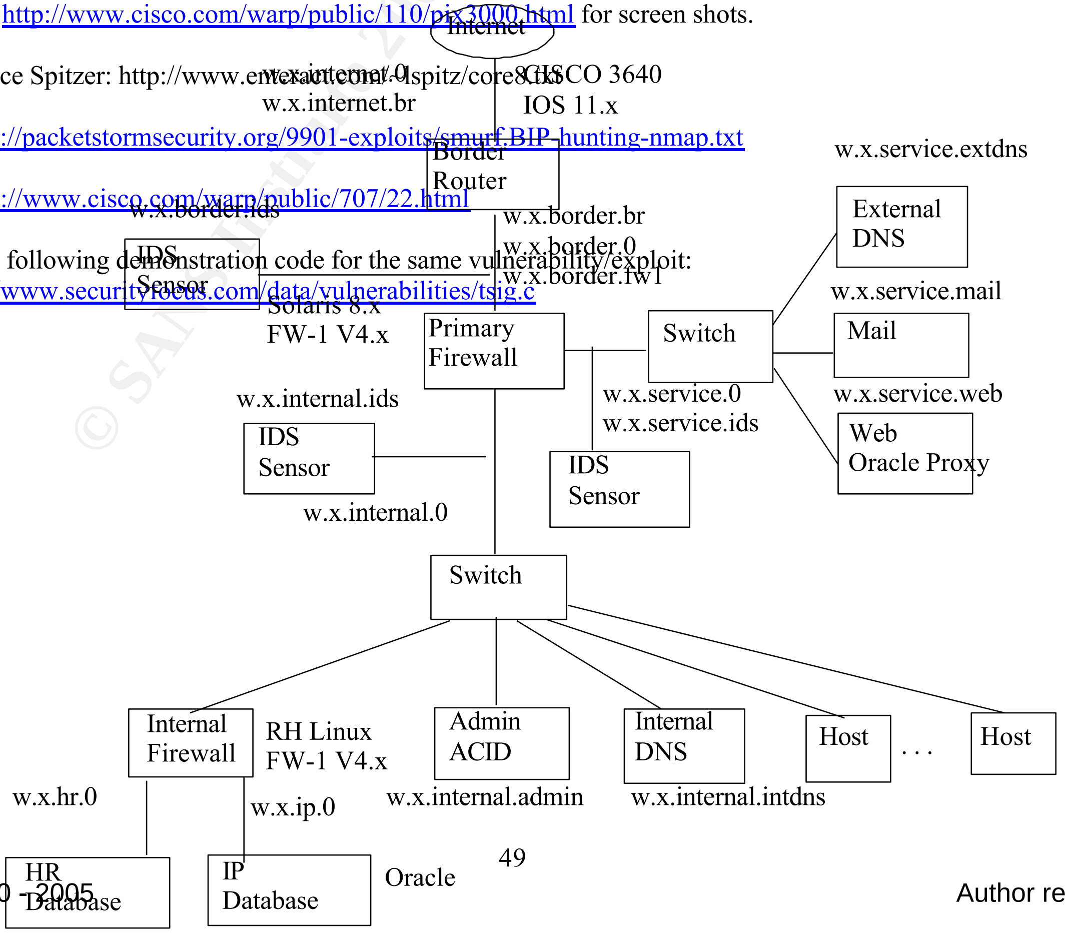
[12] See http://www.cisco.com/warp/public/110/pix3000.html for screen shots.

[13] Lance Spitzer: http://www.enteract.com/~lspitz/core8.txt

[14] http://packetstormsecurity.org/9901-exploits/smurf.BIP-hunting-nmap.txt

[15] http://www.cisco.com/warp/public/707/22.html

[16] The following demonstration code for the same vulnerability/exploit: http://www.securityfocus.com/data/vulnerabilities/tsig.c


Internet
w.x.internet.0
w.x.internet.br
CISCO 3640
IOS 11.x
Border Router
w.x.service.extdns
External DNS
w.x.border.ids
IDS Sensor
Solaris 8.x
FW-1 V4.x
w.x.border.br
w.x.border.0
w.x.border.fw1
w.x.service.mail
Primary Firewall
Switch
Mail
w.x.internal.ids
w.x.service.0
w.x.service.ids
w.x.service.web
IDS Sensor
Web Oracle Proxy
IDS Sensor
w.x.internal.0
Switch
Internal Firewall
RH Linux
FW-1 V4.x
Admin ACID
Internal DNS
Host
. . .
Host
w.x.hr.0
w.x.ip.0
w.x.internal.admin
w.x.internal.intdns
HR Database
IP Database
Oracle