Design Implementation Guide

PIX Firewall

Introduction

Cisco Systems' Private Internet Exchange Firewall (PIX™ Firewall) provides full firewall protection that completely conceals the architecture of an internal network from the outside world. PIX Firewall allows secure access to the Internet from within existing private networks and the ability to expand and reconfigure TCP/IP networks without being concerned about a shortage of IP addresses.

With PIX Firewall, users can take advantage of larger address classes than they may have been assigned by using the Network Address Translation (NAT) algorithm. NAT makes it possible to use either existing IP addresses or the addresses set aside in the Internet Assigned Numbers Authority's (IANA's) reserve pool (RFC 1597).

PIX Firewall provides "bulletproof" firewall security without the administrative overhead and risks associated with UNIX-based firewall systems. The network administrator is provided with a complete accounting and logging of all transactions, including attempted break-ins.

PIX Firewall offers controlled access to all the services of the Internet. Its streamlined software is scalable and simple to install; typical configuration takes five minutes. It offers an inexpensive, low-maintenance firewall solution that enables users to take advantage of the Internet's potential. Encryption is available with PIX Private Link to provide secure communication between multiple PIX Firewall systems over the Internet.

This document shows real-life examples of firewall configurations using PIX Firewall to completely conceal the architecture of an internal network from the outside world.

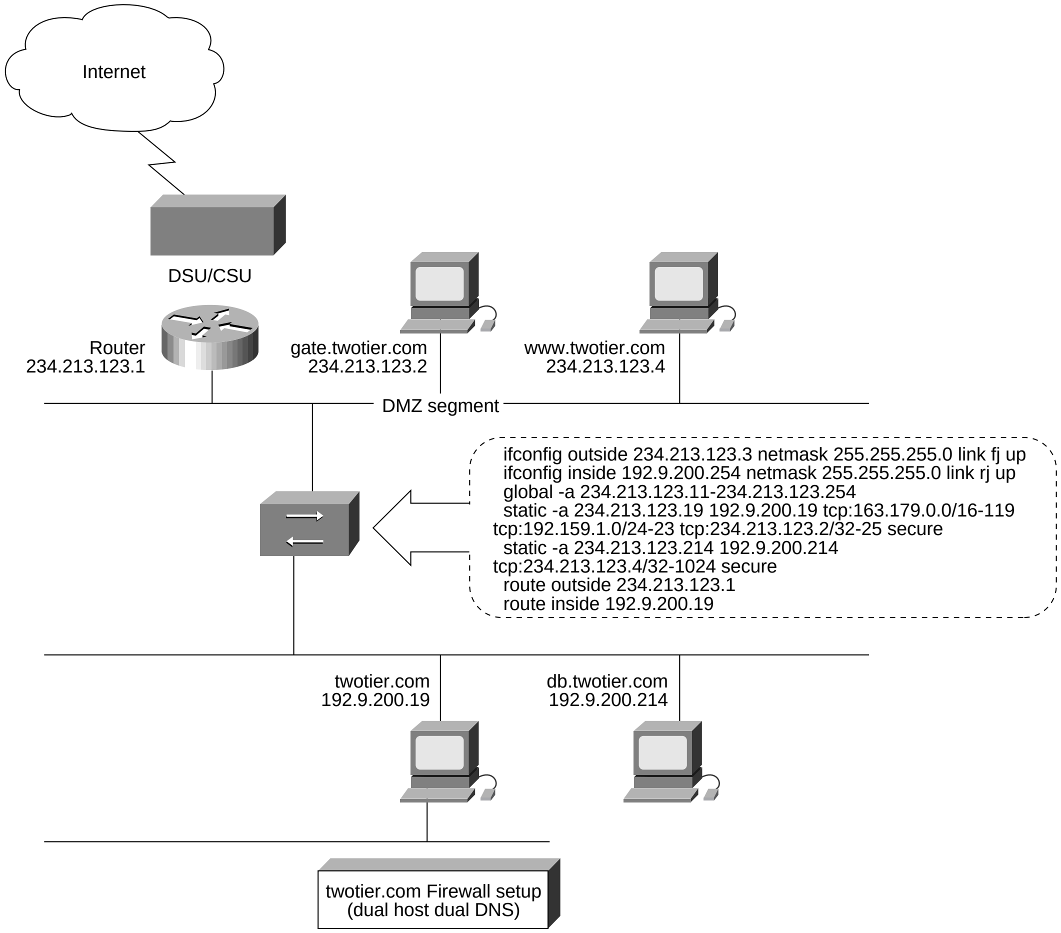
Note: This document contains data adapted from real-life installations. The names and IP addresses of the original installations have been changed to protect their confidentiality. Some configurations make security and performance trade-offs because of the limited availability of hosts for public access servers—such security shortcomings are noted in the text.

Example of a Dual DNS/Double Spooling Configuration

TWOTIER.COM

Twotier.com is probably the most desirable example of a two-tier PIX Firewall configuration. Internal and external Domain Naming Service (DNSs) are handled by separate servers, so there is no exposure of internal host names to the Internet. In addition to acting as the gateway server, gate.twotier.com serves as the File Transfer Protocol (FTP) server and mail relay. Since sendmail potentially allows security breaches, placing the mail relay host on the DMZ eliminates the risk of exposing passwords and aliases on the outside DMZ network. The Web server is set up so as to minimize the risk of damage to the host containing real data (db.twotier.com) in the event that the Web server is compromised. Figure 1 illustrates this configuration.

Figure 1. twotier.com Firewall setup (Dual Host Dual DNS)



```
  ifconfig outside 234.213.123.3 netmask 255.255.255.0 link fj up
  ifconfig inside 192.9.200.254 netmask 255.255.255.0 link rj up
  global -a 234.213.123.11-234.213.123.254
  static -a 234.213.123.19 192.9.200.19 tcp:163.179.0.0/16-119
tcp:192.159.1.0/24-23 tcp:234.213.123.2/32-25 secure
  static -a 234.213.123.214 192.9.200.214
tcp:234.213.123.4/32-1024 secure
  route outside 234.213.123.1
  route inside 192.9.200.19
```

Routing

The Internet router has a gateway of last resort at the provider's end of the WAN link, and broadcasts a default route to the DMZ segment. Both gate and WWW point their default gateway to the Internet router. No "rip outside" configuration is necessary on the PIX Firewall, since the global address pool (234.123.213.11 through 254) borrows from the DMZ. The PIX Firewall will proxy ARP for the global pool of addresses when required.

The PIX Firewall is configured to broadcast a default route to the inside. UNIX systems running in.routed (or the equivalent) need not be reconfigured to specifically point to the PIX Firewall as a default gateway. PC and Macintosh hosts must be configured to point to the PIX Firewall for a default route (unless a router is set up on the inside, in which case they should point to the internal router for a default gateway).

Whois and DNS

According to the whois database, twotier.com has the following domain servers in the order listed:

GATE.TWOTIER.COM	234.123.213.2
NS1.NOC.PROVIDER.NET	204.31.1.1
NS2.NOC.PROVIDER.NET	204.31.1.2

An MX query of twotier.com shows the following:

```
> twotier.com                    preference = 90, mail exchanger = mail.provider.com

> twotier.com                    preference = 20, mail exchanger = gate.twotier.com

> mail.provider.com internet address = 192.100.81.99

> gate.twotier.com internet address = 234.123.213.2
```

The backup MX record (mail.provider.com) facilitates inbound mail spooling from the Internet in the event that the WAN link to the provider breaks.

Bastion Host GATE.TWOTIER.COM

The following are nameserver entries for the outside DNS server in the named.zone file on gate.twotier.com.

```
gate.twotier.com.              IN        A           234.123.213.2

msmail.twotier.com.            IN        MX 20       gate.twotier.com.

msmail.twotier.com.            IN        MX 100      mail3.provider.com.

twotier.com.                   IN        MX 20       gate.twotier.com.

twotier.com.                   IN        MX 90       mail3.provider.com.

twotier.com.                   IN        A           234.123.213.19

twotier-g.twotier.com.         IN        CNAME       twotier.com.

mail.twotier.com.              IN        CNAME       twotier.com.

ftp                            IN        CNAME       gate.twotier.com.

loghost                        IN        CNAME       gate.twotier.com.

www                            IN        A           234.123.213.4

nntpserver                     IN        CNAME       gate.twotier.com.

newshost                       IN        CNAME       gate.twotier.com.

localhost.                     IN        A           127.0.0.1

c2500.twotier.com.             IN        A           234.123.213.1

; global ip addresses below

twotier3.twotier.com           IN        A           234.123.213.3

twotier5.twotier.com           IN        A           234.123.213.5

twotier6.twotier.com           IN        A           234.123.213.6

twotier7.twotier.com           IN        A           234.123.213.7

..... all the way to...

twotier251.twotier.com.        IN        A           234.123.213.251

twotier252.twotier.com         IN        A           234.123.213.252
```

```
twotier253.twotier.com      IN    A     234.123.213.253
twotier254.twotier.com.     IN    A     234.123.213.254
```

DNS Entries for the Global Cloud

The last section of the zone file contains host-name-to-IP mapping of host names corresponding to the global cloud of addresses. This setup allows access to those sites on the Internet (for example, ftp.uu.net) that require hostname verification. Be sure to set up the reverse DNS file for 213.123.234.IN-ADDR.ARPA. Refer to textbooks on DNS for further detail on the need for reverse name servers.

Revealing Internal Names for cc:mail and msmail

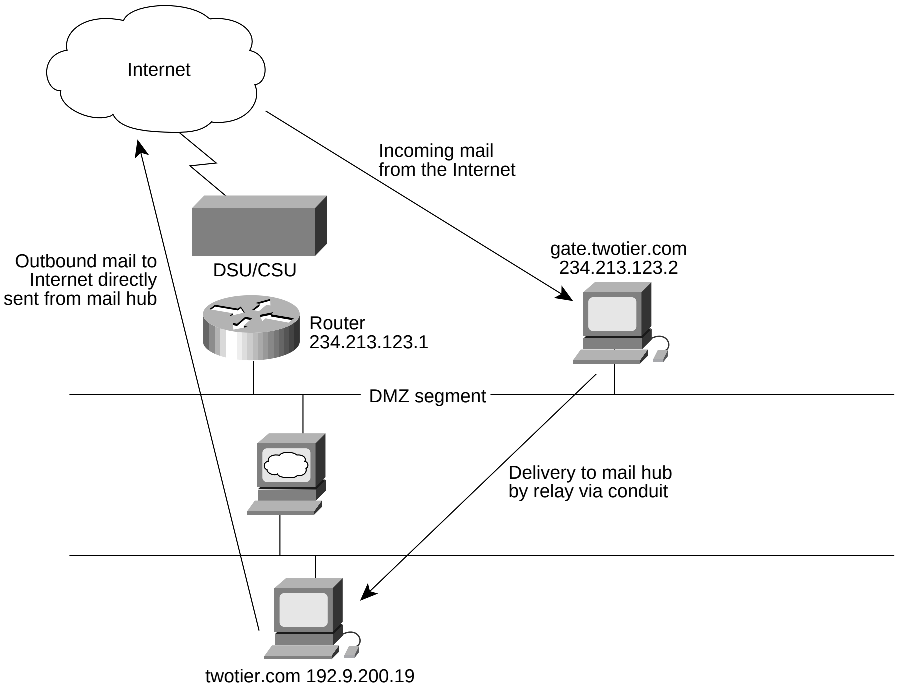
Msmail.twotier.com is revealed as an MX record. Some Internet mailers attempt to reply to the envelope instead of the “from:” address. Envelopes of messages originating from these PC mail gateways contain the host name of the gateway and are not replyable if the mailer replies to the envelope.

Consider mail originating from the internal msmail gateway that is addressed to a user on the Internet and cc’ed to an internal user. The recipient on the Internet gets a message addressed to lisa@apple.com, and cc’d to joe@msmail.twotier.com. Lisa’s reply message will also be directed to joe@msmail.twotier.com. If msmail.twotier.com does not exist as an MX record, the reply message will bounce.

Sendmail

Sendmail on the outside is configured to smart-forward to an inside host

Figure 2. gate.twotier.com uses Berkeley sendmail 8.X


Internet
Incoming mail from the Internet
Outbound mail to Internet directly sent from mail hub
DSU/CSU
gate.twotier.com 234.213.123.2
Router 234.213.123.1
DMZ segment
Delivery to mail hub by relay via conduit
twotier.com 192.9.200.19

In the example shown in Figure 2, gate.twotier.com uses Berkeley sendmail 8.X. The following is a cutout of a section of the sendmail.cf on gate:

```
# “Smart” relay host (may be null)
> DSsmtp:twotier.com
```

For details, see *ftp.translation.com:/pub/sendmail/forwarding.cf*.

An `nslookup` of twotier.com reveals an outside address, as follows:

```
> Name:    twotier.com
> Address:  234.123.213.19
```

Note: The *A* record of twotier.com is **not** an inside IP address, but a global-to-private mapping. The PIX Firewall is configured with a secure conduit for mail to be delivered only from gate.twotier.com to the internal host twotier.com.

See the MX records on gate.twotier.com. Gate smart-forwards mail addressed to either user@twotier.com or user@msmail.twotier.com to twotier.com, the inside mail host.

Zmailer

The /etc/zmailer.conf for Zmailer (**not** zmail) should look like the following:

```
ZCONFIG=/etc/zmailer.conf
HOSTENV=SunOS4.1
SHELL=/bin/sh
MAILBIN=/usr/local/lib/mail
MAILSHARE=/usr/local/share/mail
MAILVAR=/usr/local/share/mail
MAILBOX=/var/spool/mail
POSTOFFICE=/var/spool/postoffice
LOGDIR=/var/log
#LOGLEVEL=”file: recipient:”
MANDIR=/usr/local/man
#CC=gcc # gcc -Wall -pedantic
CC=cc
#COPTS=”-traditional -g”
COPTS=-g
#RANLIB=true # : ar does the work of ranlib under System V
RANLIB=ranlib # : ar does the work of ranlib under System V
INSTALL=”/usr/bin/install -o root -g bin”
NOBODY=65534
#NROUTERS=10
#MAILSERVER=yonge.cs.toronto.edu
SMTPOPTIONS=”-l /var/log/smtpserver”
PUNTHOST=twotier.com
SMARTHOST=mail3.provider.com
```

/usr/local/share/mail/db/routers should look like the following:

```
 .twotier.com                    smtp!twotier.com
```

The first field represents the domain name; the second field represents the host to which mail should be “punted” for that domain.

Internal Host TWOTIER.COM

DNS

The inside mail host is twotier.com, running DNS for the inside networks.

The following is twotier.com’s zone file:

```
 twotier.com.                  IN        A           192.9.200.19
```

msmail	IN	A	192.9.200.57
exchange	IN	A	192.9.200.179
twotier_east	IN	A	192.9.202.2
www	IN	A	234.123.213.4
gate	IN	A	234.123.213.2
news	IN	CNAME	gate.twotier.com.
twotier.com.	IN	MX 20	twotier.com.

Note: In the above DNS entry, twotier.com's MX record points to itself, so all mail is kept in /var/spool/mail unless otherwise redirected in /etc/aliases.

Sendmail

Twotier.com has a rather generic sendmail configuration, except for the rule that stamps the domain name twotier.com for outbound mail. See the following excerpts from a Berkeley sendmail v8 cf file. You can find the complete file in *ftp.translation.com:/pub/sendmail/sendmail.cf.*

```
DDtwotier.com
Dmtwotier.com
```

...CONTINUED…

S31		
R$+	$: $>51 $1	sender/recipient
common		
R$* :; <@>	$@ $1 :;	list:; special case
# do special header rewriting		
R$* <@> $*	$@ $1 <@> $2	pass null host through
R< @ $* > $*	$@ < @ $1 > $2	pass route-addr through
R$=E < @ $=w . >	$@ $1 < @ $2 >	exposed user as is
R$* < @ $* $m . >	$@ $1 < @ $m >	NTI addition
R$* < @ $=w . >	$: $1 < @ $2 @ $M >	masquerade as domain
R$* < @ $+ @ >	$@ $1 < @ $2 >	in case $M undefined
R$* < @ $+ @ $+ >	$@ $1 < @ $3 >	$M is defined --
use it		
R$*	$@ $>61 $1	qualify unqual'ed names

Twotier.com PIX Firewall Configuration

This configuration allows mail into the global map of twotier.com from gate.

Note that the outside host (www.twotier.com) can access 192.9.200.214 (the database server) via port 1024 (see the static assignments).

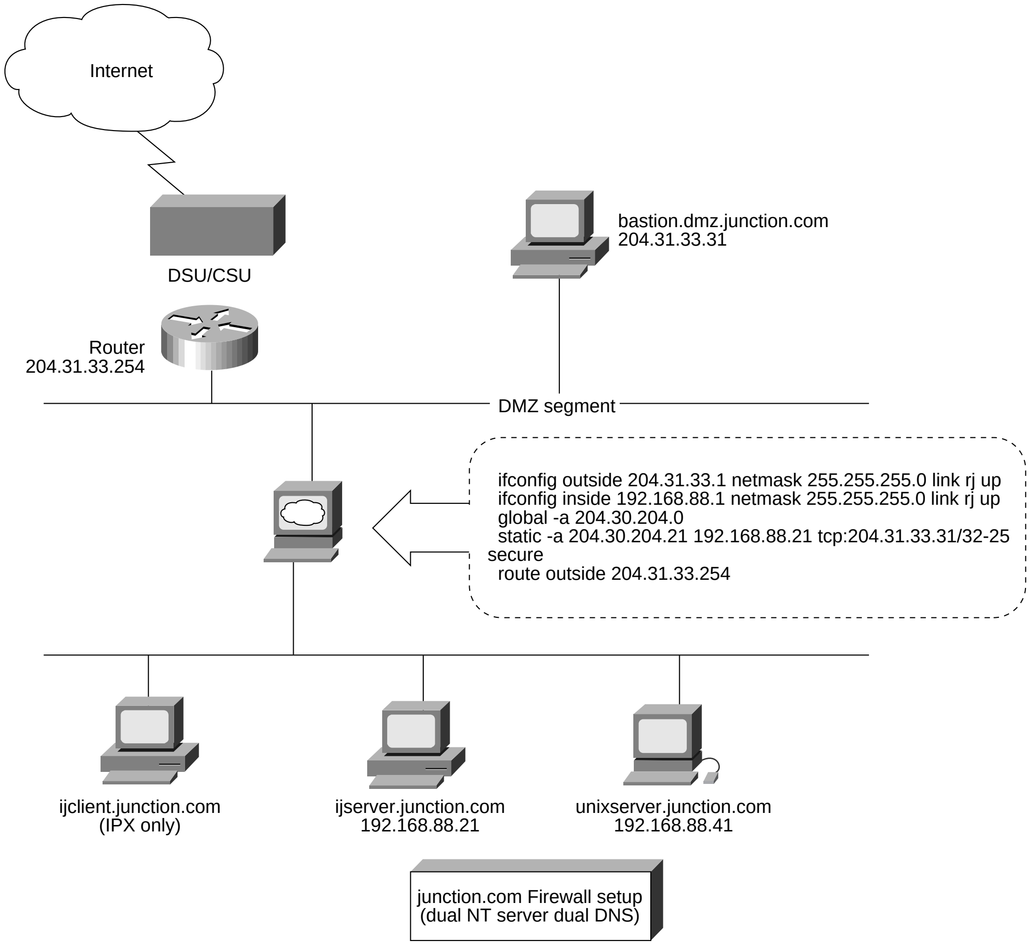
```
ifconfig outside 234.123.213.3 netmask 255.255.255.0 link rj up
ifconfig inside 192.9.200.254 netmask 255.255.255.0 link rj up
global -a 234.123.213.11-234.123.213.254
static -a 234.123.213.19 192.9.200.19 tcp:234.123.213.2/32-25 secure
static -a 234.123.213.214 192.9.200.214 tcp:234.123.213.4/32-1024 secure
route outside 234.123.213.1
route inside 192.9.200.19
timeout xlate 24:00:00 conn 12:00:00
rip inside default passive
rip outside passive
loghost 192.9.200.19
telnet 192.9.200.19
telnet 192.9.200.2
arp -t 600
```

Dual DNS Using Windows NT Gateway Hosts

Junction.com uses a Windows NT server as the gateway host and another NT server as the internal mail host. This configuration is similar to the two-tier.com example. Bastion.dmz.junction.com serves as the external DNS server, mail relay, FTP server, and Web server. Ijserver.junction.com serves as the mail host and internal DNS server.

For simplicity of network stacks management, Windows clients within junction.com do not run an IP stack. Instead, they use the Cisco Internet Junction™ IPX-to-IP protocol conversion software whose server part resides on ijserver.junction.com. With the Internet Junction software, all sessions from PC clients going out to the Internet appear as if they come from a single IP address on ijserver-g.junction.com. UNIX clients take any address assigned dynamically by the PIX Firewall.

Figure 3. junction.com Firewall Setup (Dual NT Server Dual DNS)



```
  ifconfig outside 204.31.33.1 netmask 255.255.255.0 link rj up
  ifconfig inside 192.168.88.1 netmask 255.255.255.0 link rj up
  global -a 204.30.204.0
  static -a 204.30.204.21 192.168.88.21 tcp:204.31.33.31/32-25
secure
  route outside 204.31.33.254
```

Whois and DNS

According to the whois database, junction.com has the following domain servers in the order listed:

bastion.dmz.junction.com	204.31.33.31
NS.TRANSLATION.COM	204.31.33.2
NS2.TRANSLATION.COM	204.31.33.3

An MX query of junction.com shows the following:

junction.com	preference = 10, mail exchanger = bastion.junction.com
junction.com	preference = 15, mail exchanger = gate.translation.com

Bastion Host bastion.dmz.junction.com

Bastion.dmz.junction.com is a Windows NT 3.51 server configured as follows:

Windows NT resource Kit 3.51, which provides:

- Graphical user interface (GUI)-based FTP server configuration
- A beta copy of EMWAC’s http server
- Perl 5.0.X

- Microsoft’s DNS server
- Software.com’s Post.Office sendmail package for mail relay
- NNS beta 2.06 for Usenet News services

Some alternative sources for Internet services on Windows NT include the following:

DNS

- FLBI’s DNS is available from ftp.winsite.com/pub/pc/winnt/netutils
- Software.com has a port of BIND 4.9.3

Mail

- Windows NT 3.51 Resource Kit has a point of presence (POP) server, mailsrv, with limited features
- Krypton Communications has a full-featured mail daemon/POP server package available from ftp.winsite.com/pub/pc/winnt/netutils
- Another package, NTMAIL, is available from http://www.net-shopper.co.uk/software/ntmail/

HTTPD

- Commercial Web servers for NT are available from Netscape and Oreilly and Associates

TELNETD

- telnetd is **not** recommended for security reasons

DNS

Refer to the Microsoft Windows 3.51 Resource Kit for installation instructions.

The following is a listing of the boot file in c:\winnt35\system32\drivers\etc:

```
cache       .                          cache
primary     127.in-addr.arpa.          arpa-127.rev
primary     junction.com               junction.com
primary     33.31.204.in-addr.arpa.    named.rev
primary     204.30.204.in-addr.arpa.   global.rev
```

The following is the junction.com file (note that $INCLUDE is not used here):

```
@   IN  SOA    bastion.junction.com.  postmaster.bastion.junction.com. (
                        1996031403; serial number
                        2400; refresh [3h]
                        3000; retry   [1h]
                        604800; expire  [7d]
                        86400; minimum [1d]
;;$WINS 192.5.29.2 192.5.29.3
@                       in          ns        bastion.junction.com.
@                       in          ns        ns1.translation.com.
@                       in          ns        ns2.translation.com.
bastion                 in          a         204.31.33.31
localhost               in          a         127.0.0.1
;@                      in          mx        5     ijserver.junction.com.
@                       in          mx        10     bastion.junction.com.
mail-g                  in          a         204.30.204.22
WINSsrv1                in          cname     bastion.junction.com.
ftp                     in          cname     bastion.junction.com.
www                     in          cname     bastion.junction.com.
ijserver-g              in          cname     ijserver-g.junction.com.
;
dmz                     in          cname     bastion.junction.com.
bastion.dmz             in          cname     bastion.junction.com.
host1.junction.com.     in          a         204.30.204.1
….
Host254.junction.com.   in          a         204.30.204.254
```

Note: With Krypton’s XKIMS mail server, you must configure the mail relay host bastion.dmz.junction.com to be a member of a subdomain such as dmz.junction.com to enable mail redirection to the inside host without having to use aliases. This configuration is not necessary, however, if you are using Post.Office.

Sendmail

The Internet Junction architecture achieves double spooling through the use of the bastion.dmz.junction.com mail relay. Bastion does not contain any user passwords or aliases.

Most commercial NT-based sendmail implementations (such as Post.Office) support mail redirection configuration via a GUI or a Web client.

If you are using Post.Office, the directive to enable mail forwarding to the internal mail host is configurable on the screen (Internet) message channel configuration using the following:

```
*.junction.com:ijserver-g.junction.com
```

Internal Host ijserver.junction.com

The Internal host ijserver.junction.com runs the same DNS server as the external host, but also contains information for the 192.168.88 network and 204.31.33.31.

DNS

The following is a listing of the boot file in c:\winnt35\system32\drivers\etc:

```
cache       .                           cache
primary     127.in-addr.arpa.           arpa-127.rev
primary     junction.com.               junction.com
primary     88.168.192.in-addr.arpa.    named.rev
```

The following is a listing of junction.com (note that $INCLUDE is not used here):

```
@   IN  SOA    ijserver.junction.com.  postmaster.ijserver.junction.com. (
                      1996031403; serial number
                      2400; refresh [3h]
                      3000; retry [1h]
                      604800; expire [7d]
                      86400; minimum [1d]
;;$WINS 192.5.29.2 192.5.29.3
@                     in          ns              ijserver.junction.com.
bastion               in          a               204.31.33.31
ijserver              in          a               192.168.88.21
localhost             in          a               127.0.0.1
@                     in          mx              5    ijserver.junction.com.
ftp                   in          cname           bastion.junction.com.
www                   in          cname           bastion.junction.com.
dmz                   in          cname           bastion.junction.com.
bastion.dmz           in          cname           bastion.junction.com.
unixserver            in          a               192.168.88.41
```

Sendmail

Internal sendmail uses a generic configuration, but all outbound mail must be stamped as if from [user]@junction.com. Since most mail packages for NT now support MX record lookup, there is no need for the external mail host to act as an outbound mail relay.

Junction.com PIX Firewall Configuration

The junction.com PIX Firewall has the following configuration:

```
ifconfig outside 204.31.33.1 netmask 255.255.255.0 link rj up
ifconfig inside 192.168.88.1 netmask 255.255.255.0 link rj up
global -a 204.30.204.0
static -a 204.30.204.21 192.168.88.21 tcp:204.31.33.31/32-25 secure
route outside 204.31.33.254
```

Managing the NT Bastion Using NetBIOS

For security reasons, Cisco does not recommend allowing NetBIOS over TCP/IP services to pass from bastion to ijserver. However, if such communication is required, add the following command to the PIX Firewall:

```
conduit 204.30.204.21 udp:204.31.33.31/32-137
```

This command enables the ijserver internal host to map to a shared resource on bastion.

The following command enables the external host to map a file system local to ijserver (referred to as ijserver-g in its DNS). You must preload ijserver's IP address of 204.30.204.21 in c:\winnt35\system32\drivers\etc\LMHOSTS. This setup also allows a user on bastion to log on to the Internal NT domain of JUNCTION.

Note: Cisco strongly discourages this configuration for security reasons.

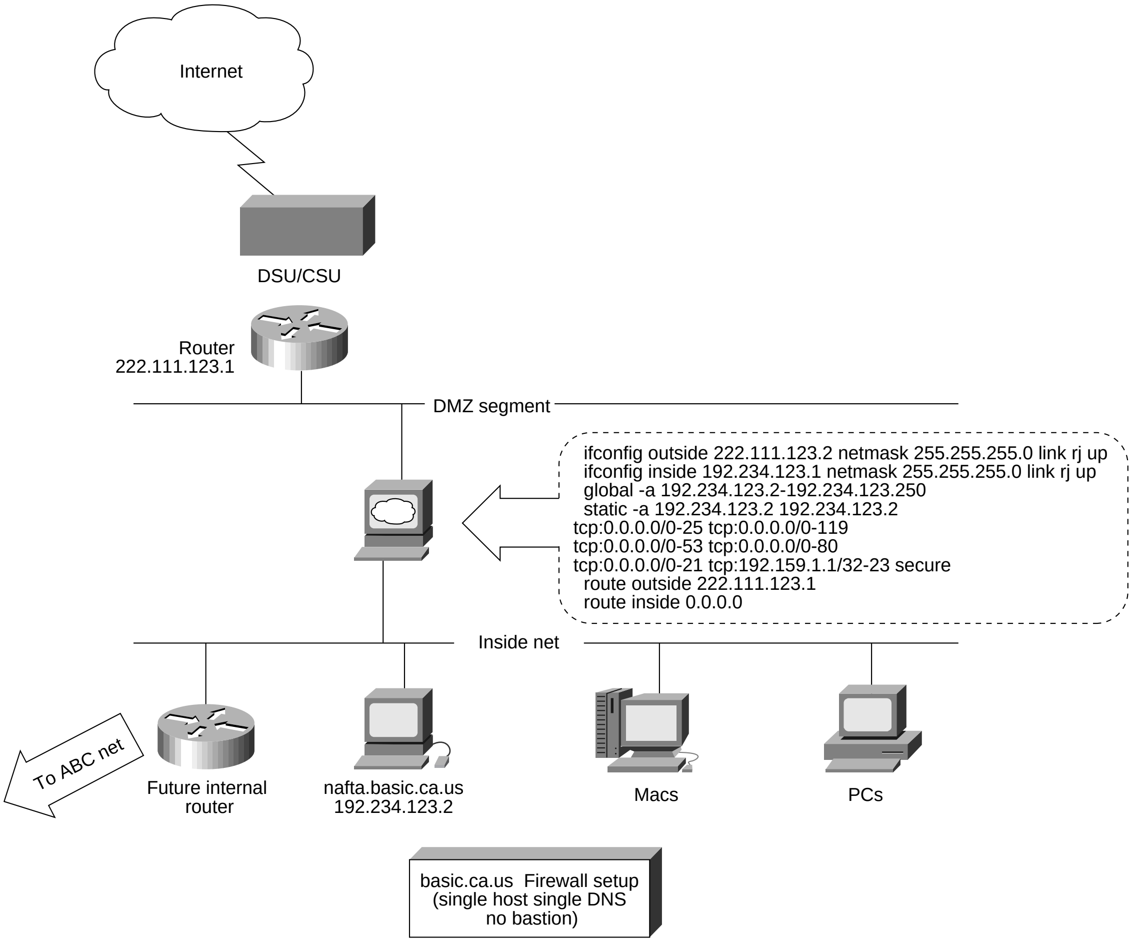
```
conduit 204.30.204.21 tcp:204.31.33.31/32-139
```

Single DNS and Mail Host Hidden Behind a PIX Firewall

Basic.ca.us has a suboptimal security configuration since the Web server/mail relay/FTP/DNS server is located inside the secure network with "holes" to which the outside world has access. There is a risk of the internal network being compromised if services like sendmail are compromised. Furthermore, the old server (nafta) contains the real "production"/etc/passwd file. If FTP is not secured in a chrooted fashion, the password file may be compromised.

Basic.ca.us has adopted this configuration because nafta is both the authoritative DNS server for basic.ca.us and the internal file server. No other UNIX host is available to serve as a bastion, and Basic.ca.us does not wish to reregister the authoritative name server to another IP address. In the future, services such as Web, FTP, and mail relay will be migrated to a bastion host on the DMZ network, leaving only DNS open to direct Internet access.

Figure 4. Basic Firewall Setup (Single Host Single DNS No Bastion)



```
  ifconfig outside 222.111.123.2 netmask 255.255.255.0 link rj up
  ifconfig inside 192.234.123.1 netmask 255.255.255.0 link rj up
  global -a 192.234.123.2-192.234.123.250
  static -a 192.234.123.2 192.234.123.2
tcp:0.0.0.0/0-25 tcp:0.0.0.0/0-119
tcp:0.0.0.0/0-53 tcp:0.0.0.0/0-80
tcp:0.0.0.0/0-21 tcp:192.159.1.1/32-23 secure
  route outside 222.111.123.1
  route inside 0.0.0.0
```

Routing

The Internet router is controlled by the Internet service provider and does not broadcast a default route via Routing Information Protocol (RIP). The PIX Firewall is configured to point to the Internet router for an outside route. Basic.ca.us uses a range of 192.234.123.2 to 250 as the global cloud; this is different from the DMZ segment (222.111.123.X).

In order to make the 192.234.123.X net visible from the Internet, a static route is configured on the Cisco 2500 Internet router to the outside interface of the PIX Firewall, as follows:

```
ip route 192.234.123.0 255.255.255.0 192.234.123.2 1
```

Technical Support Note

Ensure that the second IP address is routed to the customer’s Internet router before performing any further debugging. You can accomplish this using traceroute from the Internet to verify that both addresses (222.111.123 and 192.234.123) are routed to 222.111.123.1 (or at least to the serial interface IP of the Internet router).

Route inside 0.0.0.0 denotes no routers installed on the network inside.

Route inside can be changed to IP of internal router once it is setup.

DNS

Host nafta.basic.ca.us serves DNS to the outside and inside. The /var/named/named.boot file at Basic serves only the inside addresses (which also fully make up the global pool).

```
directory /usr/local/named
primary         basic.ca.us                     db.basic
primary         123.234.192.in-addr.arpa        db.192.234.123
primary         123.111.222.in-addr.arpa        db.222.111.123
primary         0.0.127.in-addr.arpa            db.127.0.0
cache           .                               named.ca
```

The named.zone file has some real hosts and some names for global IP addresses, as follows:

```
basic.ca.us                     IN      MX 10 nafta.basic.ca.us.
basic.ca.us.                    IN      MX 100 mail3.provider.com.
nafta.basic.ca.us.              IN      MX 10 nafta.basic.ca.us.
luna                            IN      A               192.234.123.3
moe                             IN      A               192.234.123.27
TiredMac                        IN      A               192.234.123.249
MediaPPC                        IN      A               192.234.123.250
NSC                             IN      A               192.234.123.150
nafta.basic.ca.us.              IN      A               192.234.123.2
www                             IN      CNAME           nafta.basic.ca.us.
news                            IN      CNAME           nafta.basic.ca.us.
ftp                             IN      CNAME           nafta.basic.ca.us.
ns                              IN      CNAME           nafta.basic.ca.us.

host5.basic.ca.us.              IN      A               192.234.123.5
host6.basic.ca.us.              IN      A               192.234.123.6
... all the way to ...
host252.basic.ca.us.            IN      A               192.234.123.252
host253.basic.ca.us.            IN      A               192.234.123.253
host254.basic.ca.us.            IN      A               192.234.123.254
```

Sendmail

The sendmail configuration on nafta is generic (it is similar to twotier.com). Nafta is the most preferred MX host for the basic.ca.us domain.

Basic.ca.us’s PIX Firewall Configuration

```
ifconfig 222.111.123.2 netmask 255.255.255.0 link rj up
ifconfig inside 192.234.123.1 netmask 255.255.255.0 link rj up
global -a 192.234.123.2-192.234.123.250
static -a 192.234.123.2 192.234.123.2 tcp:0.0.0.0/0-25 tcp:0.0.0.0/0-119
tcp:0.0.0.0/0-53 tcp:0.0.0.0/0-80 tcp:204.30.204.0/24-23 tcp:0.0.0.0/0-21
tcp:192.159.1.1/32-23 secure
route outside 222.111.123.1
route inside 0.0.0.0
rip inside default passive
rip outside passive
loghost 192.234.123.2
telnet 192.234.123.4
telnet 192.234.123.2
```

Note: The static here reveals the IP of nafta, which is the DNS, news, mail, Web, and FTP server. In this configuration, the inside addresses and global addresses are the same. Inside addresses are not actually revealed in this case, since outgoing connections will use IP addresses starting from 192.234.123.254 backwards and resolve back to names like host254.basic.ca.us.

DIGICORP (Another Example of a Single DNS and Mail Host Hidden Behind a PIX Firewall)

Digicorp uses the PIX Firewall to grow their network without having to acquire new addresses from their Internet Service Provider (ISP). Digicorp has their own authoritative name server and legitimate IP addresses. As part of a project to implement Internet security, Digicorp has configured a firewall similar to that of Basic. Digicorp will move Web servers to the DMZ in the future, and will add a mail relay host to further enhance Internet security.

Whois and DNS

A “whois” query of digicorp.com reveals the following:

SUN.DIGICORP.COM	204.31.17.2
PROVIDERSV.PROVIDER.COM	192.100.81.101

Digicorp.com’s PIX Firewall Configuration

The PIX Firewall will assign all hosts inside digicorp.com an IP address of 206.222.111.X when they go outside. There is only one exception—204.31.17.2 goes to the outside with its internal IP address. Digicorp thus hides all internal hosts, with the exception of the DNS server.

```
ifconfig outside 206.222.111.2 netmask 255.255.255.0 link bnc up
ifconfig inside 204.31.17.1 netmask 255.255.255.0 link bnc up
global -a 206.222.111.11-206.222.111.254
global -a 204.31.17.2-204.31.17.3
static -a 204.31.17.2 204.31.17.2 tcp:204.31.1.0/24-119
tcp:163.179.0.0/16-53 tcp:0.0.0.0/0-25 secure
route outside 206.222.111.1
route inside 204.31.17.254
```

Special Case 1—DNS Server Using Private IP Addresses

If the internal network of Digicorp uses a private or unregistered IP, and internal.digicorp.com uses 192.168.1.2, then a static should be configured as follows:

```
static -a 204.31.17.2 192.168.1.2 tcp:204.31.1.0/24-119
tcp:163.179.0.0/16-53 tcp:0.0.0.0/0-25 secure
```

Also, DNS must be set up as follows:

```
@ IN        SOA            gate-g.digidemise.com. postmaster.digicorp.com. (
                                      96011788        ; serial
                                      7200            ; refresh
                                      1800            ; retry
                                      2592000         ; expire
                                      345600)         ; Minimum
                                      IN              NS              gate-g.digicorp.com.
gate.digidemise.com.                  IN              A               192.168.88.2
gate-g                                IN              A               204.31.17.2
digidemise.com.                       IN              MX 10           gate.digicorp.com.
digidemise.com.                       IN              MX 15           gate-g.digicorp.com.
```

Special Case 2—Same IP Used on DMZ and Internal Network

When there is only one class C available from the ISP, it is still possible to use the same IP address on the outside segment/global cloud and inside network without changing the IP addresses of the internal network. A major drawback with this configuration, however, is that the outside Internet router is unmanageable from the inside LAN. In addition, hosts on the DMZ zone cannot be reached from the inside network.

If Digicorp were to use the same 204.31.17.X network, the PIX Firewall configuration would look like the following:

```
ifconfig outside 204.31.17.254 netmask 255.255.255.0 link bnc up
ifconfig inside 204.31.17.1 netmask 255.255.255.0 link bnc up
global -a 204.31.17.2-204.31.17.253
static -a 204.31.17.2 204.31.17.2 tcp:0.0.0.0/0-119 tcp:0.0.0.0/0-53
tcp:0.0.0.0/0-25 secure
route outside 204.31.17.1
route inside 204.31.17.254
```

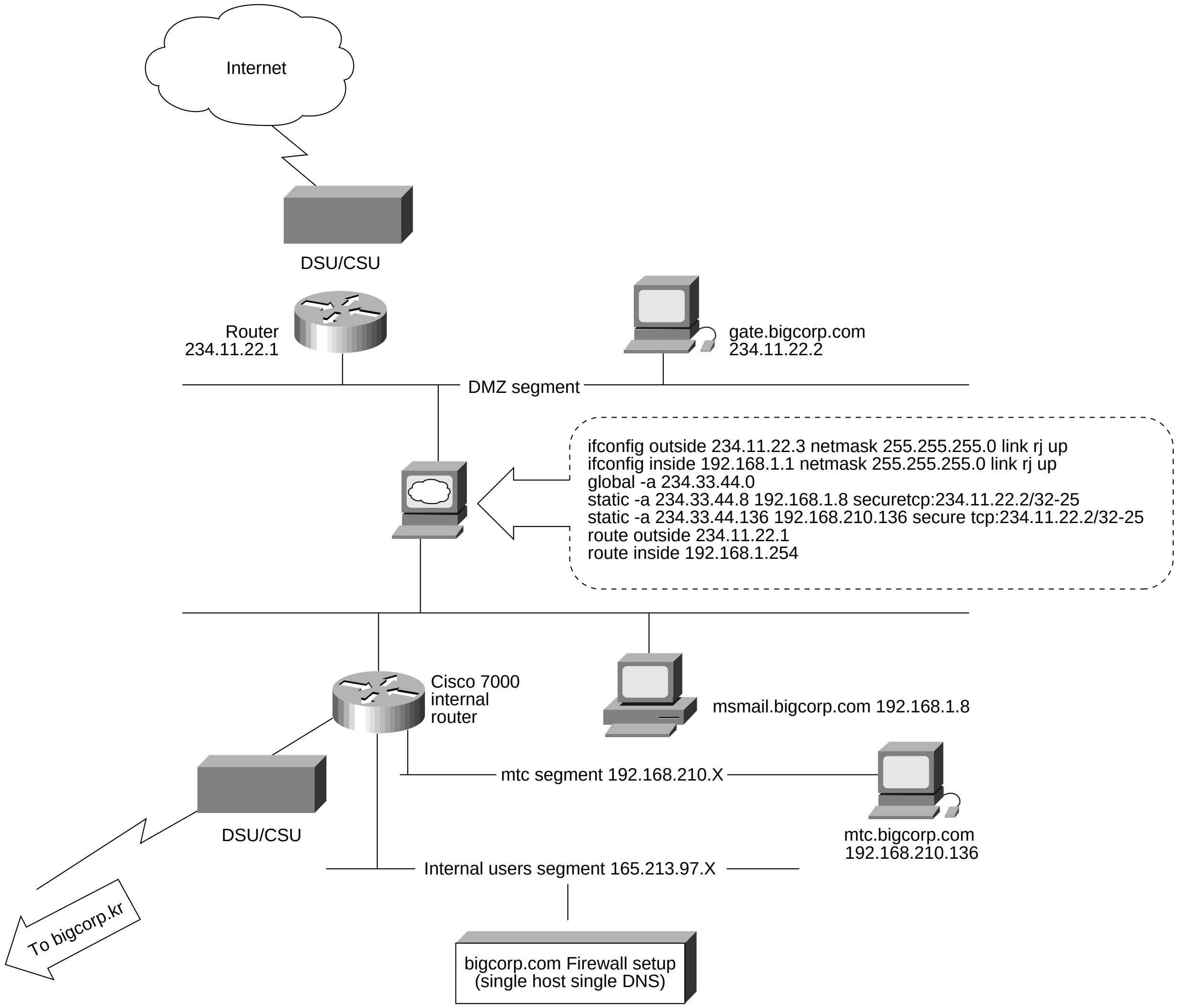
Note: As can be seen in the “static” command, only mail, DNS zone transfer, and news are open to the Internet. This configuration is suboptimal, since the Sun host, which contains passwords and aliases, is subject to direct Internet Simple Mail Transfer Protocol (SMTP) connections. The Sun host is also subject to security compromises caused by sendmail bugs.

Single Outside DNS Server Serving Outside and Inside Addresses

Bigcorp, San Jose, has a class B subnet of the Korean Bigcorp headquarters’ network configured internally. To minimize load on the T1 serving IP/IPX traffic, the router in Korea filters out access to the Internet from the San Jose network. A default route (pointing to the PIX Firewall) is configured on the Cisco 7000 to enable San Jose clients to access the Internet seamlessly.

Bigcorp must also protect the msmail SMTP gateway (which cannot handle multiple inbound connections). Unauthorized users could stall the SMTP gate by Telnetting to port 25 of msmail.bigcorp.com if it were to be exposed.

Figure 5. bigcorp.com Firewall Setup (Single Host Single DNS)



```
ifconfig outside 234.11.22.3 netmask 255.255.255.0 link rj up
ifconfig inside 192.168.1.1 netmask 255.255.255.0 link rj up
global -a 234.33.44.0
static -a 234.33.44.8 192.168.1.8 securetcp:234.11.22.2/32-25
static -a 234.33.44.136 192.168.210.136 secure tcp:234.11.22.2/32-25
route outside 234.11.22.1
route inside 192.168.1.254
```

Routing

The outside DMZ zone (234.11.22.0) has a different IP address than the global cloud (234.33.44.0). A static route on the Internet router routes 234.33.44.X to 234.11.22.3. The Internal Cisco 7000 has a default gateway set to 192.168.1.1.

Whois and DNS

Whois on bigcorp.com shows authoritative name servers as follows:

NS1.NOC.PROVIDER.NET	204.31.1.1
NS2.NOC.PROVIDER.NET	204.31.1.2

However, nslookup shows that the SOA belongs to the host gate.bigcorp.com:

```
jma.com% nslookup
Default Server:  jma.com
Address:  192.159.1.1

> set q=soa
> bigcorp.com
Server:  jma.com
Address:  192.159.1.1

bigcorp.com
        origin = gate.bigcorp.com
        mail addr = postmaster.bigcorp.com
        serial = 96020102
        refresh = 1800 (30 mins)
        retry   = 900 (15 mins)
        expire  = 2592000 (30 days)
        minimum ttl = 345600 (4 days)
bigcorp.com                 nameserver = gate.bigcorp.com
bigcorp.com                 nameserver = ns1.noc.provider.net
bigcorp.com                 nameserver = ns2.noc.provider.net
gate.bigcorp.com                    internet address = 234.11.22.2
ns1.noc.provider.net                internet address = 204.31.1.1
ns2.noc.provider.net                internet address = 204.31.1.2
```

Gate.bigcorp.com is the actual primary DNS server, with ns1.noc.provider.net and ns2.noc.provider.net serving as secondary servers, periodically transferring zone files from gate.bigcorp.com.

Gate.bigcorp.com's zone file looks like the following:

```
gate.bigcorp.com.          IN     A        234.11.22.2
bigcorp.com.               IN     MX 20    gate.bigcorp.com.
bigcorp.com.               IN     MX 60    mail2.provider.com.
ftp                        IN     CNAME    gate.bigcorp.com.
loghost                    IN     CNAME    gate.bigcorp.com.
www                        IN     A        203.241.132.36
nntpserver                 IN     CNAME    gate.bigcorp.com.
newshost                   IN     CNAME    gate.bigcorp.com.
localhost.                 IN     A        127.0.0.1
irx                        IN     A        234.11.22.1
msmail                     IN     A        234.33.44.8
msmail.bigcorp.com.        IN     MX 10    msmail.bigcorp.com.
msmail.bigcorp.com.                 IN    MX 90    gate.bigcorp.com.
abcipo.msmail.bigcorp.com.          IN    MX 20    msmail.bigcorp.com.
abcipo.msmail.bigcorp.com.          IN    MX 30    gate.bigcorp.com.
ssi.bigcorp.com.                    IN    MX 20    msmail.bigcorp.com.
ssi.bigcorp.com.                    IN    MX 30    gate.bigcorp.com.
hub                                 IN    A        192.168.1.3
master.bigcorp.com.                 IN    A        192.168.210.136
```

Sendmail for msmail.bigcorp.com and Related Post Offices

In this configuration, mail “trickles” through to the msmail smtpgate from the Internet, as follows:

First, mail from outside will attempt to connect to:

```
abcipo.msmail.bigcorp.com.          IN    MX 20    msmail.bigcorp.com.
```

and fail; then it resorts to:

```
abcipo.msmail.bigcorp.com.          IN    MX 30    gate.bigcorp.com.
```

This trickling occurs for all other msmail post offices configured as subdomains, as well as the subdomain mtc.bigcorp.com., which we will discuss later on.

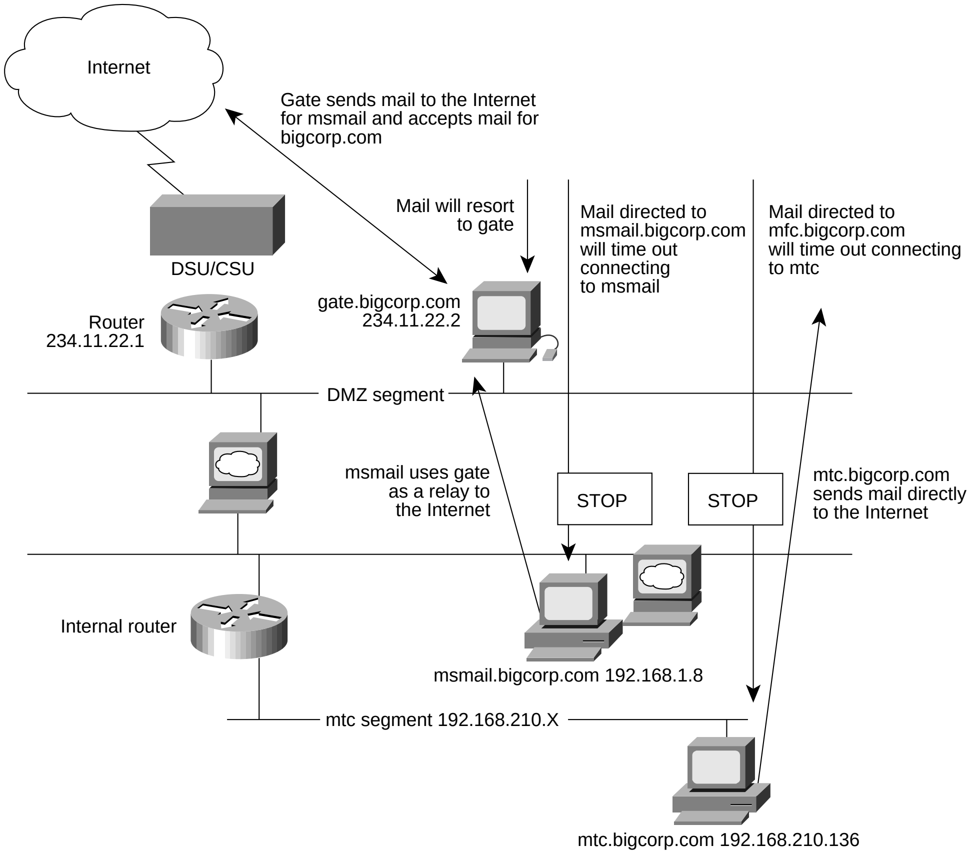
A Note About This Mail Configuration

Gate.bigcorp.com's sendmail is not modified to do any special rewriting since msmail.bigcorp.com relies on gate to pass outbound messages. If gate is configured to smart-forward mail to msmail as in the two-tier example, a mail loop results.

If we place a UNIX host that can be used as a mail relay inside or on the DMZ, we can eliminate this awkward mail setup. The resulting configuration would use gate as the MX host for all *.bigcorp.com domains, smart-forward mail to the UNIX host inside Bigcorp’s network, and fan out mail to the different mail servers internally.

As an alternative, we could install Zmailer on gate.bigcorp.com. Zmailer will intelligently route mail addressed to user@msmail.bigcorp.com, user@abcipo.msmail.bigcorp.com, and any subdomains on msmail to the msmail SMTP gateway. Zmailer will intelligently route outbound Internet messages for msmail without looping.

Figure 6.


Internet
Gate sends mail to the Internet for msmail and accepts mail for bigcorp.com
DSU/CSU
Router 234.11.22.1
Mail will resort to gate
gate.bigcorp.com 234.11.22.2
Mail directed to msmail.bigcorp.com will time out connecting to msmail
Mail directed to mfc.bigcorp.com will time out connecting to mtc
DMZ segment
msmail uses gate as a relay to the Internet
STOP
STOP
mtc.bigcorp.com sends mail directly to the Internet
Internal router
msmail.bigcorp.com 192.168.1.8
mtc segment 192.168.210.X
mtc.bigcorp.com 192.168.210.136

Gate.bigcorp.com's named.boot serves all legitimate, private, and bogus addresses, as follows:

```
directory                          /var/named
xfrnets                            204.31.1.0
cache                              . named.ca
primary bigcorp.com                named.zone
primary ssi.bigcorp.com            ssi.bigcorp.com
primary 226.30.204.in-addr.arpa    named.rev
primary 61.33.204.in-addr.arpa     global.rev
primary 1.168.192.in-addr.arpa     inside.rev
primary 210.168.192.in-addr.arpa   mtc.rev
primary 97.213.165.in-addr.arpa    165.rev
primary 97.213.174.in-addr.arpa    174.rev
primary 0.0.127.in-addr.arpa       local.rev
```

The following entries in the inside.zone file cover the private addresses inside:

```
inside1.bigcorp.com.        IN     A     192.168.1.1
inside2.bigcorp.com.        IN     A     192.168.1.2
inside3.bigcorp.com.        IN     A     192.168.1.3
inside4.bigcorp.com.        IN     A     192.168.1.4
inside5.bigcorp.com.        IN     A     192.168.1.5
inside6.bigcorp.com.        IN     A     192.168.1.6
```

Sendmail for Subdomain Mail Hosts

The following configuration applies to subdomains inside the Bigcorp firewall (such as MTC.bigcorp.com) that have their own UNIX mail host:

```
> set q=MX
> mtc.bigcorp.com
Server: gate.bigcorp.com
Address: 234.11.22.2
```

```
mtc.bigcorp.com preference = 10, mail exchanger = master.bigcorp.com
mtc.bigcorp.com preference = 20, mail exchanger = abc-g.bigcorp.com
mtc.bigcorp.com preference = 30, mail exchanger = gate.bigcorp.com
master.bigcorp.com          internet address = 192.168.210.136
abc-g.bigcorp.com           internet address = 234.33.44.136
gate.bigcorp.com            internet address = 234.11.22.2
```

Note: Abc-g.bigcorp.com is a static map of 192.168.210.136 and has a conduit for mail delivery only from gate.bigcorp.com, since the sendmail daemon of master.bigcorp.com is not security-enhanced.

Normally, only the following entries are required in DNS:

```
mtc.bigcorp.com preference = 20, mail exchanger = abc-g.bigcorp.com
mtc.bigcorp.com preference = 30, mail exchanger = gate.bigcorp.com
abc-g.bigcorp.com               internet address = 234.33.44.136
gate.bigcorp.com                internet address = 234.11.22.2
```

However, master.bigcorp.com runs Sun sendmail.mx, which blindly follows MX records. If the entry

```
mtc.bigcorp.com preference = 10, mail exchanger = master.bigcorp.com
```

is omitted, mail reaching master.bigcorp.com will loop to its global address (the most preferred MX host), which it can never reach (since a machine cannot ping its global address from the inside). The mail subsequently loops back to gate.bigcorp.com, based on the MX records on gate.bigcorp.com.

```
mtc.bigcorp.com preference = 20, mail exchanger = abc-g.bigcorp.com
mtc.bigcorp.com preference = 30, mail exchanger = gate.bigcorp.com
```

Note: You can avoid this awkward sendmail problem by using ZMAILER (not zmail) on gate.bigcorp.com or Berkeley sendmail on all inside hosts.

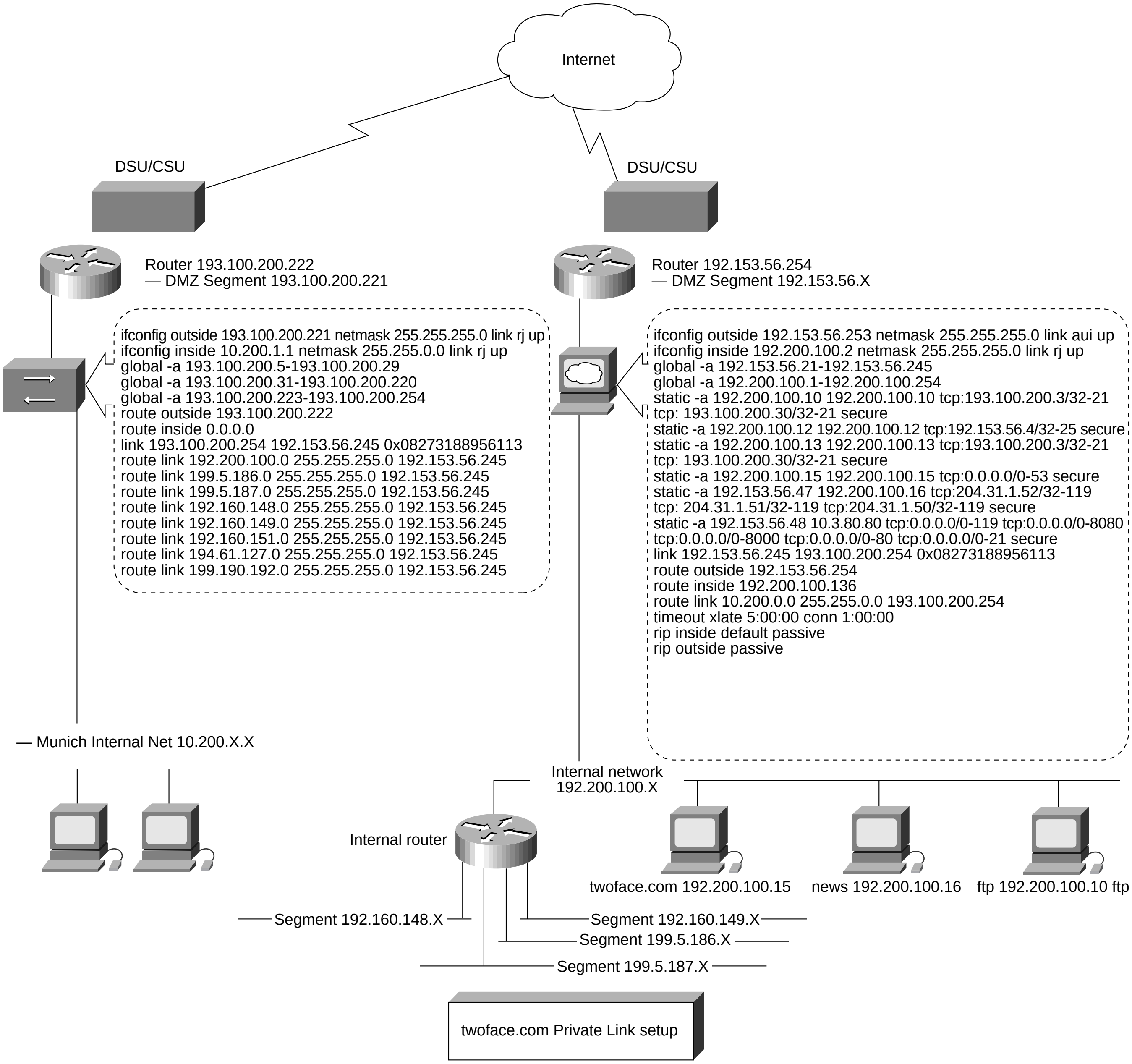
Bigcorp.com’s PIX Firewall Configuration

```
ifconfig outside 234.11.22.254 netmask 255.255.255.0 link rj up
ifconfig inside 192.168.1.1 netmask 255.255.255.0 link rj up
global -a 234.33.44.1-234.33.44.254
static -a 234.33.44.8 192.168.1.8 tcp:234.11.22.2/32-25 secure
static -a 234.33.44.136 192.168.210.136 tcp:234.11.22.2/32-25 secure
static -a 234.33.44.145 192.168.1.145 tcp:234.11.22.2/32-25 secure
route outside 234.11.22.1
route inside 192.168.1.3
timeout xlate 1:00:00 conn 12:00:00
rip inside default passive
rip outside nonpassive
loghost 0.0.0.0
telnet 192.168.210.136
telnet 234.11.22.2
telnet 192.168.202.253
telnet 192.168.1.253
arp -t 600
: version 2.7.1
```

PIX Private Link Example

Twoface.com has multiple sites connected via PIX Private Link. Like Digicorp and basic.ca.us, twoface has public access servers both on the DMZ and behind the PIX Firewall. These public access servers are accessed from the Internet via static conduits.

Figure 7. twoface.com Private Link Setup



```
ifconfig outside 193.100.200.221 netmask 255.255.255.0 link rj up
ifconfig inside 10.200.1.1 netmask 255.255.0.0 link rj up
global -a 193.100.200.5-193.100.200.29
global -a 193.100.200.31-193.100.200.220
global -a 193.100.200.223-193.100.200.254
route outside 193.100.200.222
route inside 0.0.0.0
link 193.100.200.254 192.153.56.245 0x08273188956113
route link 192.200.100.0 255.255.255.0 192.153.56.245
route link 199.5.186.0 255.255.255.0 192.153.56.245
route link 199.5.187.0 255.255.255.0 192.153.56.245
route link 192.160.148.0 255.255.255.0 192.153.56.245
route link 192.160.149.0 255.255.255.0 192.153.56.245
route link 192.160.151.0 255.255.255.0 192.153.56.245
route link 194.61.127.0 255.255.255.0 192.153.56.245
route link 199.190.192.0 255.255.255.0 192.153.56.245
```

```
ifconfig outside 192.153.56.253 netmask 255.255.255.0 link aui up
ifconfig inside 192.200.100.2 netmask 255.255.255.0 link rj up
global -a 192.153.56.21-192.153.56.245
global -a 192.200.100.1-192.200.100.254
static -a 192.200.100.10 192.200.100.10 tcp:193.100.200.3/32-21
tcp: 193.100.200.30/32-21 secure
static -a 192.200.100.12 192.200.100.12 tcp:192.153.56.4/32-25 secure
static -a 192.200.100.13 192.200.100.13 tcp:193.100.200.3/32-21
tcp: 193.100.200.30/32-21 secure
static -a 192.200.100.15 192.200.100.15 tcp:0.0.0.0/0-53 secure
static -a 192.153.56.47 192.200.100.16 tcp:204.31.1.52/32-119
tcp: 204.31.1.51/32-119 tcp:204.31.1.50/32-119 secure
static -a 192.153.56.48 10.3.80.80 tcp:0.0.0.0/0-119 tcp:0.0.0.0/0-8080
tcp:0.0.0.0/0-8000 tcp:0.0.0.0/0-80 tcp:0.0.0.0/0-21 secure
link 192.153.56.245 193.100.200.254 0x08273188956113
route outside 192.153.56.254
route inside 192.200.100.136
route link 10.200.0.0 255.255.0.0 193.100.200.254
timeout xlate 5:00:00 conn 1:00:00
rip inside default passive
rip outside passive
```

DNS

twoface.com	NS	twoface.com
twoface.com	NS	NS1.NOC.PROVIDER.NET
twoface.com	NS	NS2.NOC.PROVIDER.NET
twoface.com	A	192.200.100.15

Note: Before Twoface configured the firewall, twoface.com had a valid IP address. The firewall configuration approximately follows that of basic.com and digicorp.com.

Twoface Sunnyvale Site PIX Firewall Configuration

```
ifconfig outside 192.200.101.253 netmask 255.255.255.0 link aui up
ifconfig inside 192.200.100.2 netmask 255.255.255.0 link rj up
global -a 192.200.101.21-192.200.101.245
global -a 192.200.100.1-192.200.100.254
static -a 192.200.100.10 192.200.100.10 tcp:193.100.200.3/32-21 tcp:193.100.200.30/32-21 secure
static -a 192.200.100.12 192.200.100.12 tcp:192.200.101.4/32-25 secure
static -a 192.200.100.13 192.200.100.13 tcp:193.100.200.3/32-21 tcp:193.100.200.30/32-21 secure
static -a 192.200.100.15 192.200.100.15 tcp:0.0.0.0/0-53 secure
static -a 192.200.101.47 192.200.100.16 tcp:204.31.1.52/32-119 tcp:204.31.1.51/32-119
  tcp:204.31.1.50/32-119 secure
static -a 192.200.101.48 10.3.80.80 tcp:0.0.0.0/0-119 tcp:0.0.0.0/0-8080 tcp:0.0.0.0/0-8000
  tcp:0.0.0.0/0-80 tcp:0.0.0.0/0-21 secure
link 192.200.101.245 193.100.200.254 0x08273188956113
route outside 192.200.101.254
route inside 192.200.100.136
route link 10.200.0.0 255.255.0.0 193.100.200.254
timeout xlate 5:00:00 conn 1:00:00
rip inside default passive
rip outside passive
```

Twoface Zurich Site PIX Firewall Configuration

This site has one flat network, as follows:

```
ifconfig outside 193.100.200.221 netmask 255.255.255.0 link rj up
ifconfig inside 10.200.1.1 netmask 255.255.0.0 link rj up
global -a 193.100.200.5-193.100.200.29
global -a 193.100.200.31-193.100.200.220
global -a 193.100.200.223-193.100.200.254
route outside 193.100.200.222
route inside 0.0.0.0
link 193.100.200.254 192.200.101.245 0x08273188956113
route link 192.200.100.0 255.255.255.0 192.200.101.245
route link 199.5.186.0 255.255.255.0 192.200.101.245
route link 199.5.187.0 255.255.255.0 192.200.101.245
route link 192.160.148.0 255.255.255.0 192.200.101.245
route link 192.160.149.0 255.255.255.0 192.200.101.245
route link 192.160.151.0 255.255.255.0 192.200.101.245
route link 194.61.127.0 255.255.255.0 192.200.101.245
route link 199.190.192.0 255.255.255.0 192.200.101.245
```

Note: There are multiple “route link” commands setting up routes from the Zurich network to almost all internal networks at the Sunnyvale site.

Syslog

This section provides examples of syslog files generated on a Sun SPARCstation running SunOS 4.1.4.

The following is a cutout of /etc/syslog.conf: (Be sure to use tabs instead of spaces in this file.)

```
local4.crit         /var/log/pix/security
local5.err          /var/log/pix/resource
local6.notice       /var/log/pix/system
local7.info         /var/log/pix/acct
```

The following is a directory listing of /var/log/pix:

```
inside.sinai-balt.com% ls -la
total 53484
drwxr-sr-x  2 root            512 Jun 14  1995 .
drwxr-sr-x  4 root            512 Feb 10 04:05 ..
-rw-r--r--  1 root            54359851 Feb 15 20:00 acct
-rw-r--r--  1 root            306741 Feb 15 19:58 resource
-rw-r--r--  1 root            40450 Feb 14 08:11 security
-rw-r--r--  1 root            1878 Jan  3 16:41 system
```

Annotated Examples of PIX Firewall Logs

acct

The following line records the start of an SMTP (25) connection from 204.33.212.2 to 21.84.5.1 via a the global address 204.33.212.4:

```
Feb 15 19:56:44 pixin  conn start faddr 204.33.212.2 fport 2485  gaddr 204.33.212.4 laddr 21.84.5.1
lport 25
```

The following line records the end of the same connection with information on byte count transferred:

```
Feb 15 19:56:50 pixin  conn end faddr 204.33.212.2 fport 2485 gaddr
204.33.212.4 laddr 21.84.5.1 lport 25 duration 0:00:06 bytes 3672
```

The following line logs the start an outbound mail sent from 21.84.5.1:

```
Feb 15 20:00:28 pixin  conn start faddr 198.69.28.2 fport 25  gaddr 204.33.212.4 laddr 21.84.5.1
lport 1721
```

The following line logs the end of another outbound mail connection:

```
Feb 15 20:00:35 pixin  conn end faddr 198.69.28.2 fport 25 gaddr 204.33.212.4 laddr 21.84.5.1 lport
1700 duration 0:02:09 bytes 0
```

The following line logs the start of a connection to a Web server on the Internet from 21.84.5.1:

```
Feb 15 20:06:00 pixin  conn start faddr 17.254.3.61 fport 80  gaddr 204.33.212.4 laddr 21.84.5.1
lport 1787
```

acct.txt Generated from WIN95 Syslog32

An example of the acct.txt file generated by pixlog32 follows. The other files—security.txt, resource.txt, and system.txt—are the same as their UNIX syslog counterparts. Note that host names are resolved based on IP addresses and displayed in the log files.

```
Mar 7 11:6:47     192.168.88.252     Accounting (23)     Informational (6)     conn end faddr
204.31.17.3 fport 21 gaddr 204.30.204.252 laddr 192.168.88.141 lport 1274 duration 0:20:01 bytes 1438
Mar 7 11:7:22     192.168.88.252     Accounting (23)     Informational (6)     conn end faddr
```

```
204.31.17.3 (ns.snoopy.com) fport 23 (telnet) gaddr 204.30.204.252 laddr 192.168.88.141 (johnson-pc.translation.com) lport
1272 (Unknown Service) duration 0:21:36 bytes 1864

Mar 7 11:7:23     192.168.88.252     Accounting (23)     Informational (6)     conn start faddr

204.31.17.3 (ns.snoopy.com) fport 23 (telnet) gaddr 204.30.204.252 laddr 192.168.88.141 (johnson-pc.translation.com) lport
1284 (Unknown Service)

Mar 7 11:7:58     192.168.88.252     Accounting (23)     Informational (6)     conn end faddr

204.31.17.3 (ns.snoopy.com) fport 23 (telnet) gaddr 204.30.204.252 laddr 192.168.88.141 (johnson-pc.translation.com) lport
1284 (Unknown Service) duration 0:00:34 bytes 319

Mar 7 11:11:22    192.168.88.252     Accounting (23)     Informational (6)    conn start faddr

204.30.228.2 (gate.usdla.org) fport 3641 (Unknown Service) gaddr 204.30.204.21 laddr 192.168.88.21
(ntilocal.translation.com) lport 119 (nntp)

Mar 7 11:13:5     192.168.88.252     Accounting (23)     Informational (6)     conn start faddr

204.31.33.1 (gate.translation.com) fport 2718 (Unknown Service) gaddr 204.30.204.3 laddr 192.168.88.3 (pao.translation.com)
lport 25 (smtp)

Mar 7 11:13:21    192.168.88.252     Accounting (23)     Informational (6)     conn end faddr

204.31.33.1 (gate.translation.com) fport 2718 (Unknown Service) gaddr 204.30.204.3 laddr 192.168.88.3 (pao.translation.com)
lport 25 (smtp) duration 0:00:16 bytes 3742
```

Security

Sendmail uses port 113 for IDENT purposes. Since the PIX Firewall is blocking IDENT, we see apparent violations to port 113 on host 192.234.123.252. You can safely ignore these apparent violations.

```
Feb  1 13:43:12 pix-in  deny tcp out 202.255.181.6 4739 in 192.234.123.252
113  flags SYN
Feb  1 13:43:24 pix-in  deny tcp out 202.247.130.38 1446 in 192.234.123.252
113  flags SYN
```

The following line is a log of an attempt to Telnet to port 23 of 192.234.123.2 from 204.30.228.2:

```
Feb 15 18:09:52 pix-in deny tcp out 204.30.228.2 4042 in 192.234.123.2 23  flags SYN
```

Resource

The resource file reports at 15-minute intervals on issues such as license usage.

```
Feb  1 13:11:15 pix-in  conns 256 conns_used 2 xlate 249 xlate_used 16
Feb  1 13:24:11 pix-in  conns 256 conns_used 2 xlate 249 xlate_used 16
Feb  1 13:37:02 pix-in  conns 256 conns_used 4 xlate 249 xlate_used 16
```

Note: The first four fields (`Feb  1 13:37:02 pix-in`) are not part of the PIX Firewall output. These fields are prepended by the syslog daemon on the UNIX log host.

Some UNIX systems append an “ERR” string after the time field, which sometimes misleads users to believe that the PIX Firewall has an error.

The PIX Firewall sends warning messages to syslog upon reaching 80 percent or higher usage of the connection license.

```
Feb 12 09:36:24 twoface-gw  PIX out of connections! 24/256
```

System

This system file logs Telnet access:

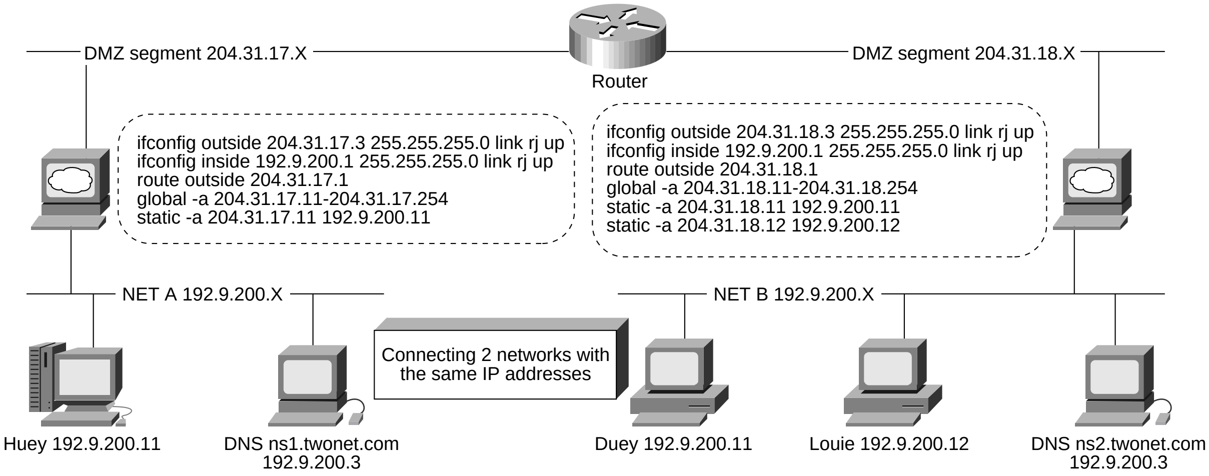
```
Feb  1 13:56:14 pix-in  PIX logged out at 192.234.123.2
Feb  1 14:00:28 pix-in  PIX logged in from 192.234.123.2
Feb  1 14:00:55 pix-in  PIX logged out at 192.234.123.2
```

Note: In this example, Telnet to the PIX Firewall is allowed only from 192.234.123.2.

Special Application: Connecting Networks with the Same IP Addresses

Twonet.com has two networks with the same 192.9.200.X addresses. Normally, it would be impossible to connect the two networks without changing the address of one network. However, using two PIX Firewalls and two DNS servers, we can allow hosts to talk to servers on the other side of the network.

Figure 8. Connecting Two Networks with the Same IP Addresses



```
ifconfig outside 204.31.17.3 255.255.255.0 link rj up
ifconfig inside 192.9.200.1 255.255.255.0 link rj up
route outside 204.31.17.1
global -a 204.31.17.11-204.31.17.254
static -a 204.31.17.11 192.9.200.11
```

```
ifconfig outside 204.31.18.3 255.255.255.0 link rj up
ifconfig inside 192.9.200.1 255.255.255.0 link rj up
route outside 204.31.18.1
global -a 204.31.18.11-204.31.18.254
static -a 204.31.18.11 192.9.200.11
static -a 204.31.18.12 192.9.200.12
```

DNS for Network A Name Server

NS1 is the name server for network A. The named.boot file looks like the following:

directory	/var/named	
cache	.	named.ca
primary twonet.com	named.zone	
primary 192.9.200.in-addr.arpa	named.rev	
primary 17.31.204.in-addr.arpa	global.rev	

named.zone contains entries for:

ns1	IN	A	192.9.200.3
huey	IN	A	192.9.200.11
duey	IN	A	204.31.18.11
louie	IN	A	204.31.18.12

named.rev contains entries for:

```
3          IN        PTR       ns1.twonet.com.
11         IN        PTR       huey.twonet.com.
```

global.rev contains:

```
11         IN        PTR       huey.twonet.com.
```

as well as entries for dynamic mappings:

```
12         IN        PTR       a12.twonet.com.
……
254        IN        PTR       a254.twonet.com.
```

DNS for Network B Name Server

NS2 is the name server for network B. The named.boot file looks like the following:

```
directory                             /var/named
cache                                 .     named.ca
primary twonet.com                    named.zone
primary 192.9.200.in-addr.arpa        named.rev
primary 18.31.204.in-addr.arpa        global.rev
```

Named.zone contains entries for:

```
ns2        IN        A        192.9.200.3
huey       IN        A        204.31.17.11
duey       IN        A        192.9.200.11
louie      IN        A        192.9.200.12
```

Named.rev contains entries for:

```
3          IN        PTR       ns1.twonet.com.
11         IN        PTR       duey.twonet.com.
12         IN        PTR       louie.twonet.com.
```

Global.rev contains:

```
11         IN        PTR       duey.twonet.com.
12         IN        PTR       louie.twonet.com.
```

as well as entries for dynamic mappings:

```
13                 IN            PTR            b13.twonet.com.

……all the way thru

254                IN            PTR            a254.twonet.com.
```

Note: The file named.ca in named.boot is the official cache file containing entries of the root name servers provided by ftp.internic.net. Therefore, access to the Internet will still be seamless.

PIX Firewall Configuration for Network A

```
ifconfig outside 204.31.17.3 255.255.255.0 link rj up
ifconfig inside 192.9.200.1 255.255.255.0 link rj up
route outside 204.31.17.1
global -a 204.31.17.11-204.31.17.254
static -a 204.31.17.11 192.9.200.11
```

PIX Firewall Configuration for Network B

```
ifconfig outside 204.31.18.3 255.255.255.0 link rj up
ifconfig inside 192.9.200.1 255.255.255.0 link rj up
route outside 204.31.18.1
global -a 204.31.18.11-204.31.18.254
static -a 204.31.18.11 192.9.200.11
static -a 204.31.18.12 192.9.200.12
```

Note: Statics are not required except for servers to which clients on the other network require access.

Issues with Simple Network Management Protocol

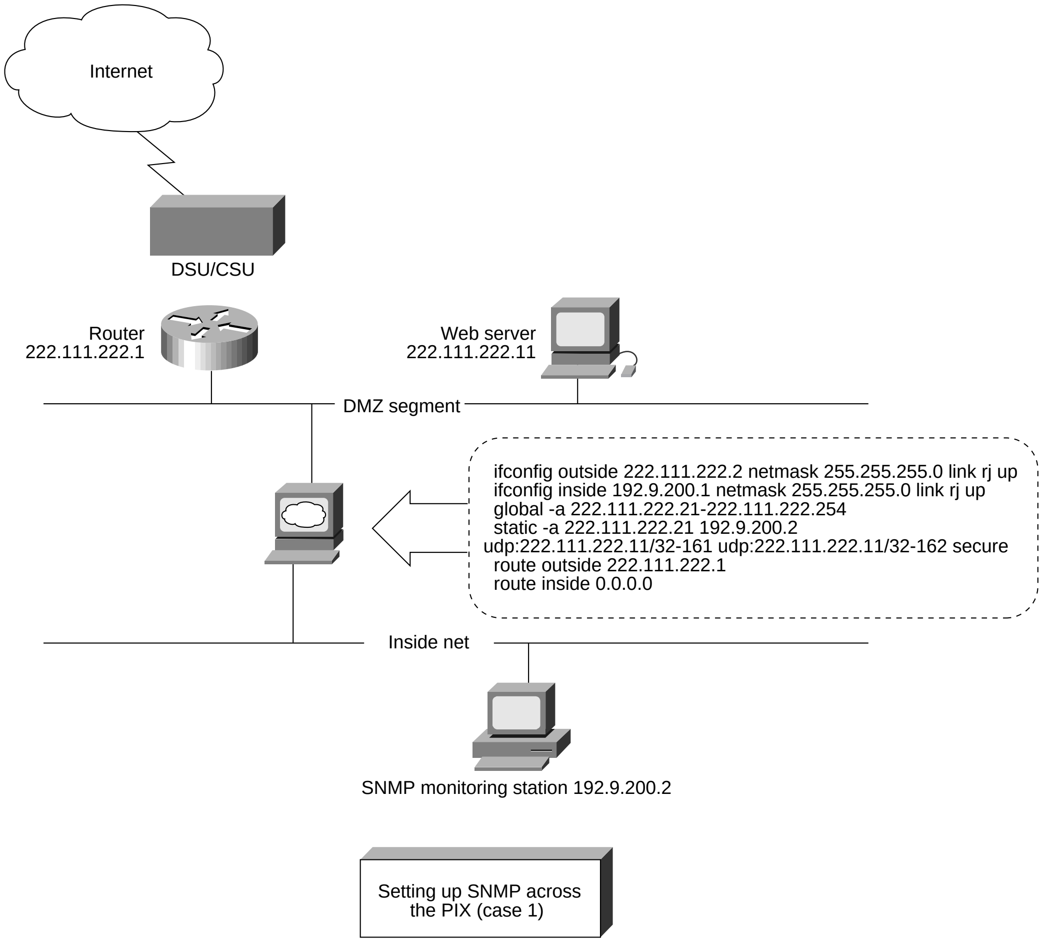
Configuring Simple Network Management Protocol/Extended Remote Monitoring Across the PIX Firewall

The PIX Firewall itself does not support Simple Network Management Protocol (SNMP) as a manageable device.

The following cases describe how devices can be managed across the PIX Firewall.

SNMP Case 1

Figure 9. Setting Up SNMP across the PIX Firewall (Case 1)

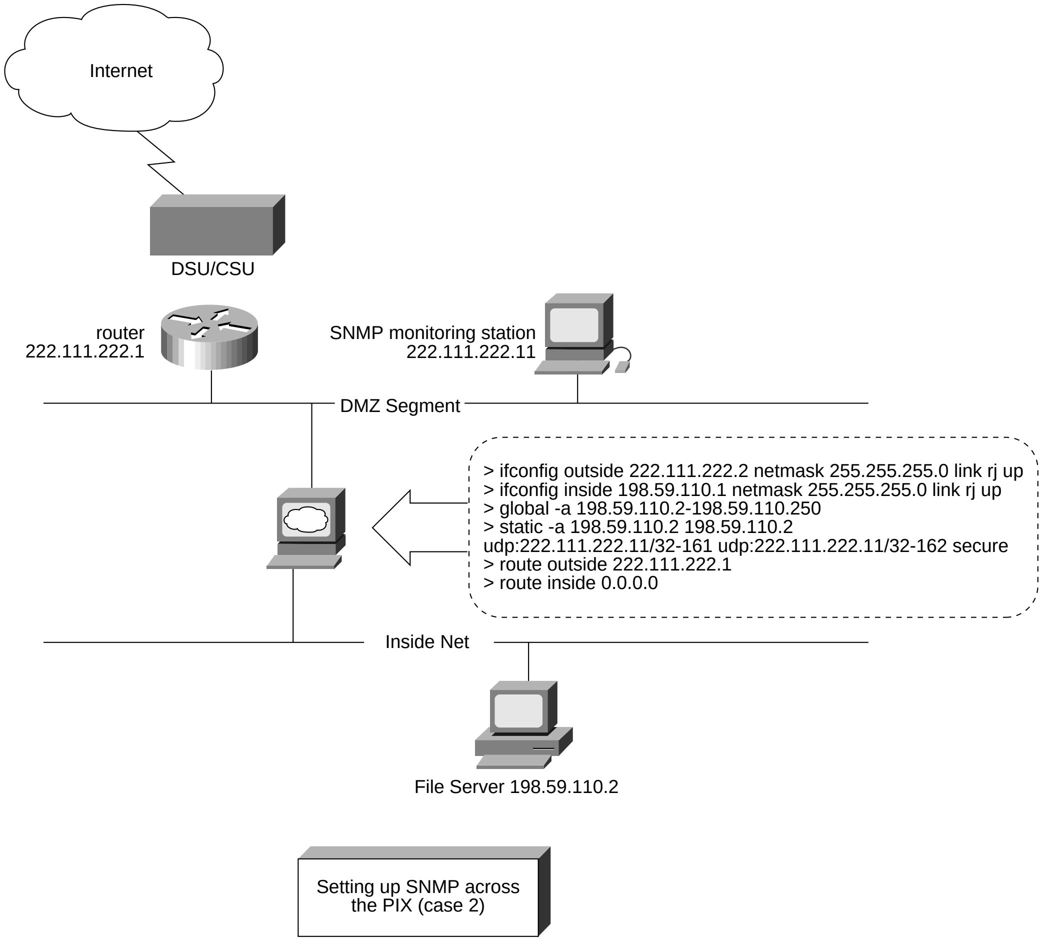


```
  ifconfig outside 222.111.222.2 netmask 255.255.255.0 link rj up
  ifconfig inside 192.9.200.1 netmask 255.255.255.0 link rj up
  global -a 222.111.222.21-222.111.222.254
  static -a 222.111.222.21 192.9.200.2
udp:222.111.222.11/32-161 udp:222.111.222.11/32-162 secure
  route outside 222.111.222.1
  route inside 0.0.0.0
```

In Figure 9, an SNMP monitoring station inside manages a Web server on the outside. A conduit is required for 222.111.222.2 to pass the SNMP traps to 192.9.200.2.

SNMP Case 2

Figure 10. Setting Up SNMP across the PIX Firewall (Case 2)

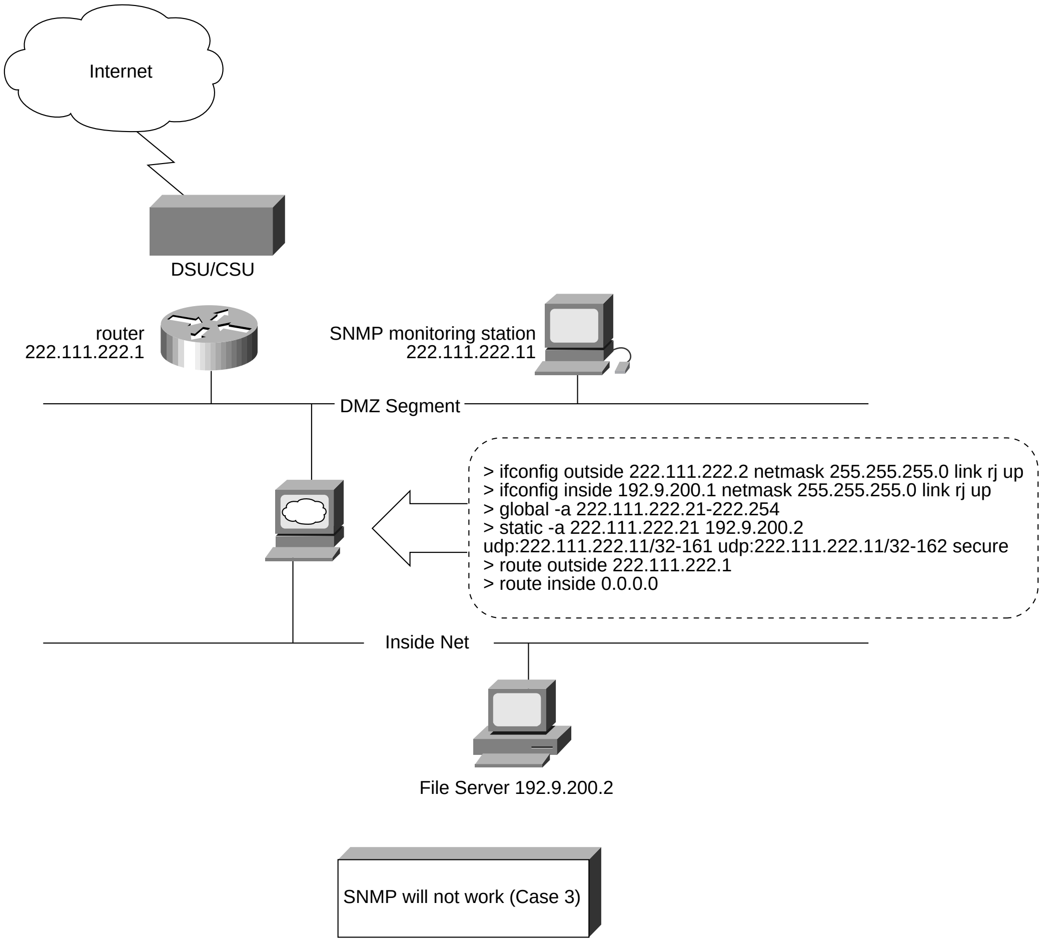


```
> ifconfig outside 222.111.222.2 netmask 255.255.255.0 link rj up
> ifconfig inside 198.59.110.1 netmask 255.255.255.0 link rj up
> global -a 198.59.110.2-198.59.110.250
> static -a 198.59.110.2 198.59.110.2
udp:222.111.222.11/32-161 udp:222.111.222.11/32-162 secure
> route outside 222.111.222.1
> route inside 0.0.0.0
```

In Figure 10, the outside SNMP monitoring station manages the file server on the Internal network. The inside network must have a legitimate IP address so that the static translation for the file server is the same as the IP address of the server itself. The source IP address of the SNMP packet sent by the file server will be consistent with the IP address described in the SNMP data.

SNMP Case 3

Figure 11. SNMP Will Not Work (Case 3)



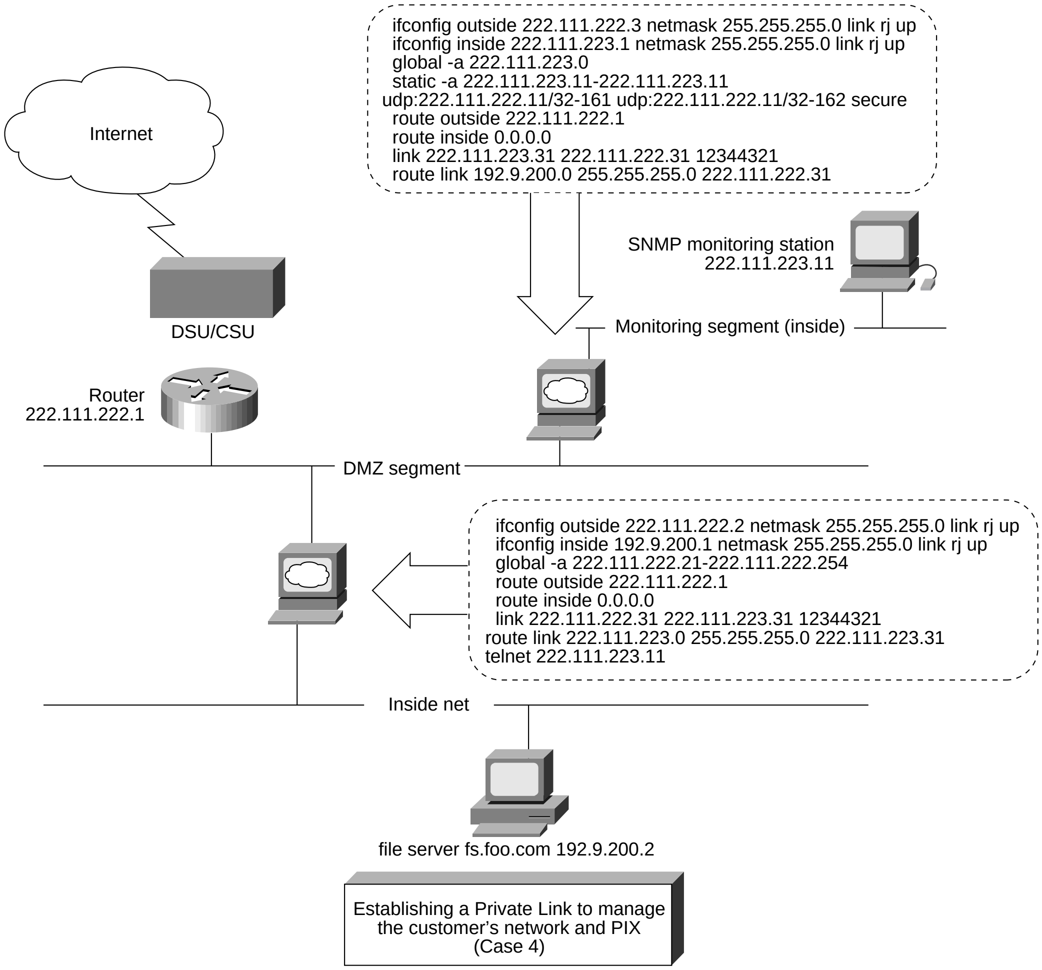
```
> ifconfig outside 222.111.222.2 netmask 255.255.255.0 link rj up
> ifconfig inside 192.9.200.1 netmask 255.255.255.0 link rj up
> global -a 222.111.222.21-222.254
> static -a 222.111.222.21 192.9.200.2
udp:222.111.222.11/32-161 udp:222.111.222.11/32-162 secure
> route outside 222.111.222.1
> route inside 0.0.0.0
```

In Figure 11, the SNMP monitoring station will see an SNMP packet from 222.111.222.21 rather than from 192.9.200.2. This address is inconsistent with the address in the SNMP-protocol data unit (PDU) header of a trap PDU, and with the address in a varbind in the varbindlist.

SNMP Case 4

In contrast with Case 3, if a PIX Private Link is used between the management station and the server, the network 192.9.200.X will be recognized as an immediate neighbor with no access restrictions. SNMP will work because the IP source of the packet from 192.9.200.2 will be received with no address modification. Additionally, the monitoring workstation can manage the PIX Firewall used at the customer site

Figure 12. Establishing a Private Link to Manage the Customer's Network and PIX Firewall (Case 4)



```
ifconfig outside 222.111.222.3 netmask 255.255.255.0 link rj up
ifconfig inside 222.111.223.1 netmask 255.255.255.0 link rj up
global -a 222.111.223.0
static -a 222.111.223.11-222.111.223.11
udp:222.111.222.11/32-161 udp:222.111.222.11/32-162 secure
route outside 222.111.222.1
route inside 0.0.0.0
link 222.111.223.31 222.111.222.31 12344321
route link 192.9.200.0 255.255.255.0 222.111.222.31
```

```
ifconfig outside 222.111.222.2 netmask 255.255.255.0 link rj up
ifconfig inside 192.9.200.1 netmask 255.255.255.0 link rj up
global -a 222.111.222.21-222.111.222.254
route outside 222.111.222.1
route inside 0.0.0.0
link 222.111.222.31 222.111.223.31 12344321
route link 222.111.223.0 255.255.255.0 222.111.223.31
telnet 222.111.223.11
```

Internet
DSU/CSU
Router
222.111.222.1
SNMP monitoring station
222.111.223.11
Monitoring segment (inside)
DMZ segment
Inside net
file server fs.foo.com 192.9.200.2
Establishing a Private Link to manage
the customer's network and PIX
(Case 4)

In Case 4, shown in Figure 12, you must configure a reverse DNS entry for 200.9.192.IN-ADDR.ARPA for the file server on the monitoring station to ensure that the name resolved from 192.9.200.2 is fs.foo.com and not the real owner of 192.9.200.X out on the Internet.

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
World Wide Web URL:
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Cisco Systems has more than 125 sales offices worldwide. To contact your local account representative, call Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).
0196R