Firewalls:

Designing a Secure Environment

October 14, 2002

Jennifer L. Bayuk
Bear Stearns & Co., Inc
jbayuk@bear.com

Firewalls can be used to:

Corral – fence a set of computers within a secure network

Expose – open gates in the fence

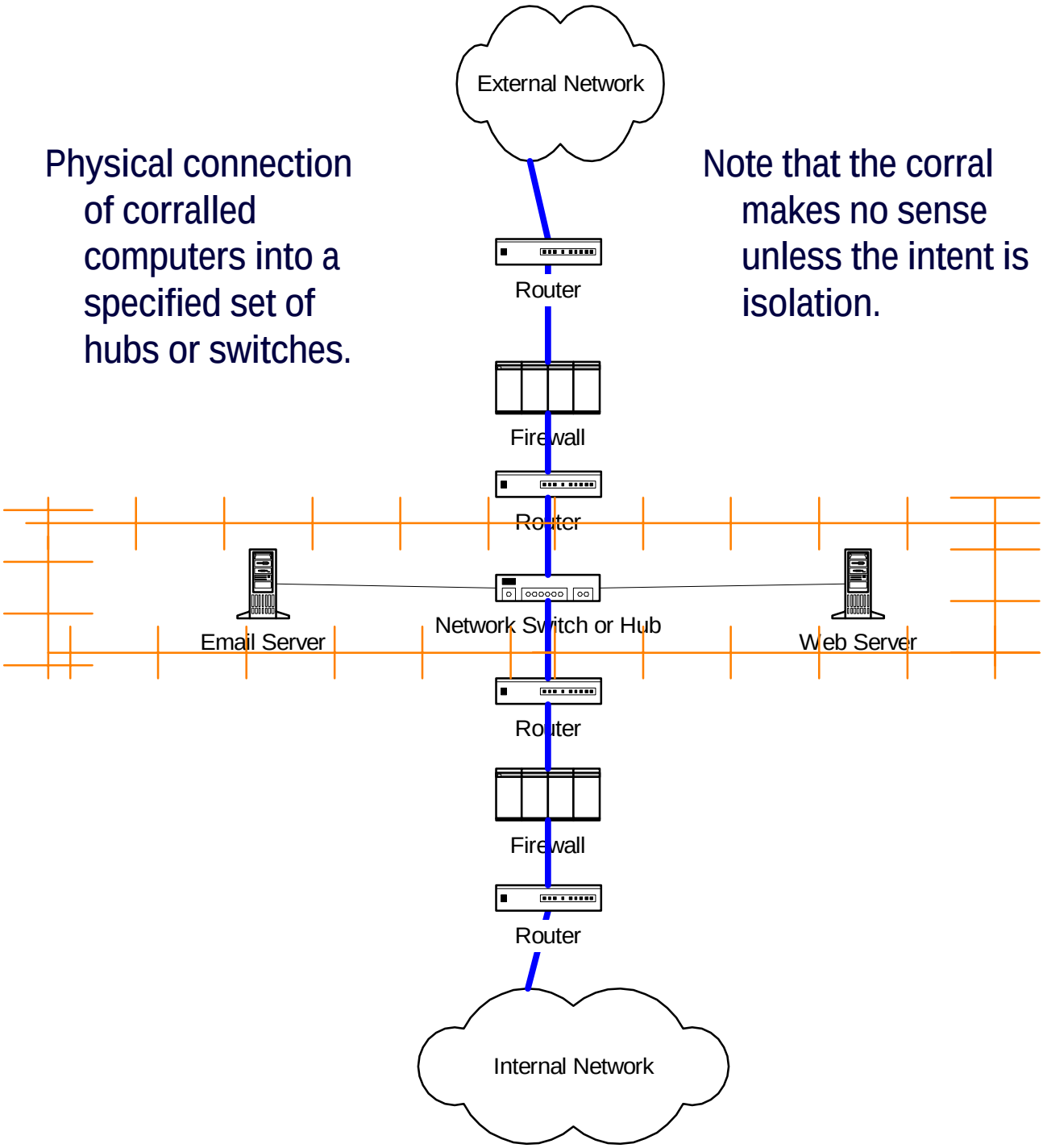
Hide – prevent access through the gates via combinations locks where the combinations are network addresses and protocols

Broker – further control some gates by requiring the approval of an external system before opening the locks

Corral Example 1

Physical connection of corralled computers into a specified set of hubs or switches.

Note that the corral makes no sense unless the intent is isolation.



Expose

Routers - traffic direction, network address, protocol

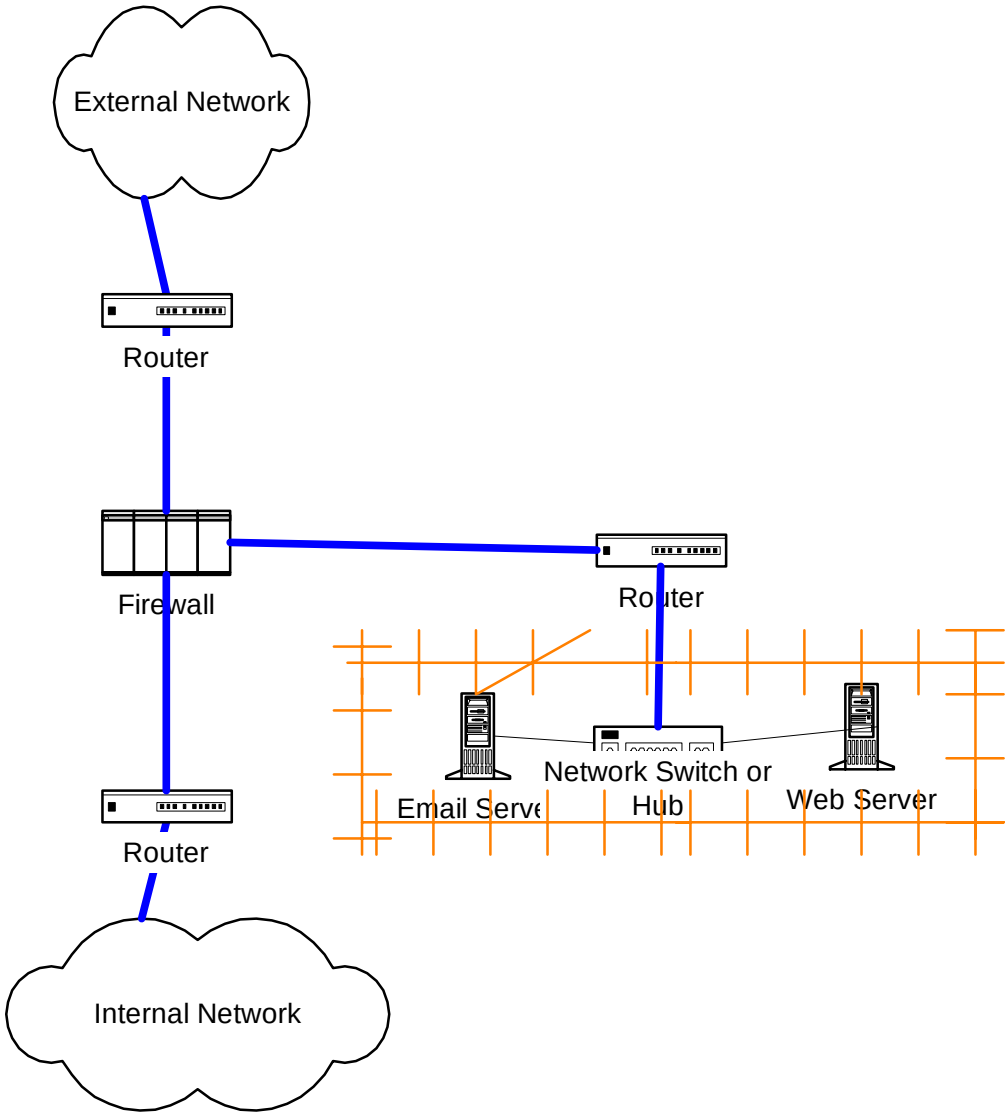
DESTINATION: 209.34.123.0 (e.g. internal net)
NEXT HOP: 209.20.73.5
DEFAULT: 122.35.28.3 (e.g. internet)

SOURCE: 163.27.130.2
DESTINATION: 209.34.123.71
PROTOCOL: TCP PORT 21
SOURCE: 209.34.123.71
DESTINATION: 163.27.130.2
PROTOCOL : TCP PORT 20, TCP PORT >1021

Firewalls – network address and service, session tracking

SOURCE: 163.27.130.2
DESTINATION: 209.34.123.71
SERVICE: FTP
TRACK: LONG LOG

Corral Example 2



Hide

Network route filters

Network traffic filters

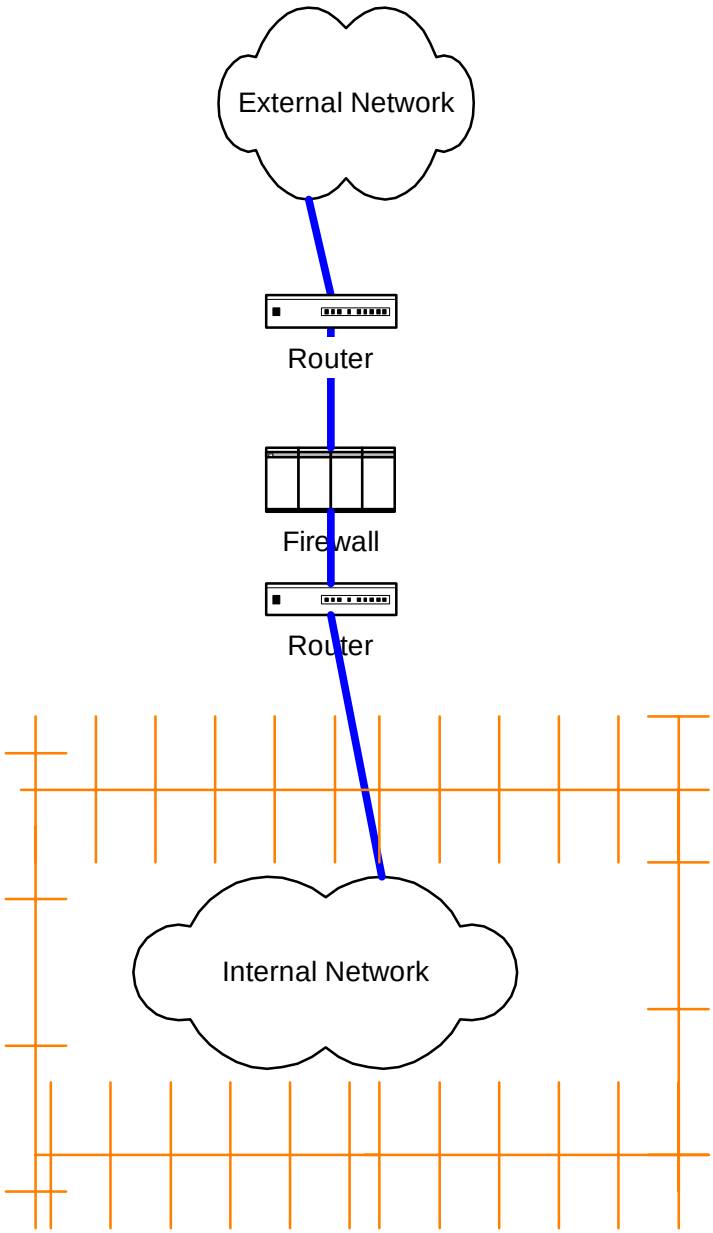
No broadcast features (e.g. hubs, multicast protocols)

No advertising features (e.g. DNS or other directory services)

Network address translation

Note that you do not need a corral to hide, only to hide selectively. Physical isolation will work to hide completely.

Corral Example 3



Broker

Authentication Servers – when faced with firewalls, pass certain combinations of traffic, firewall requires user identification and authorization prior to initializing session

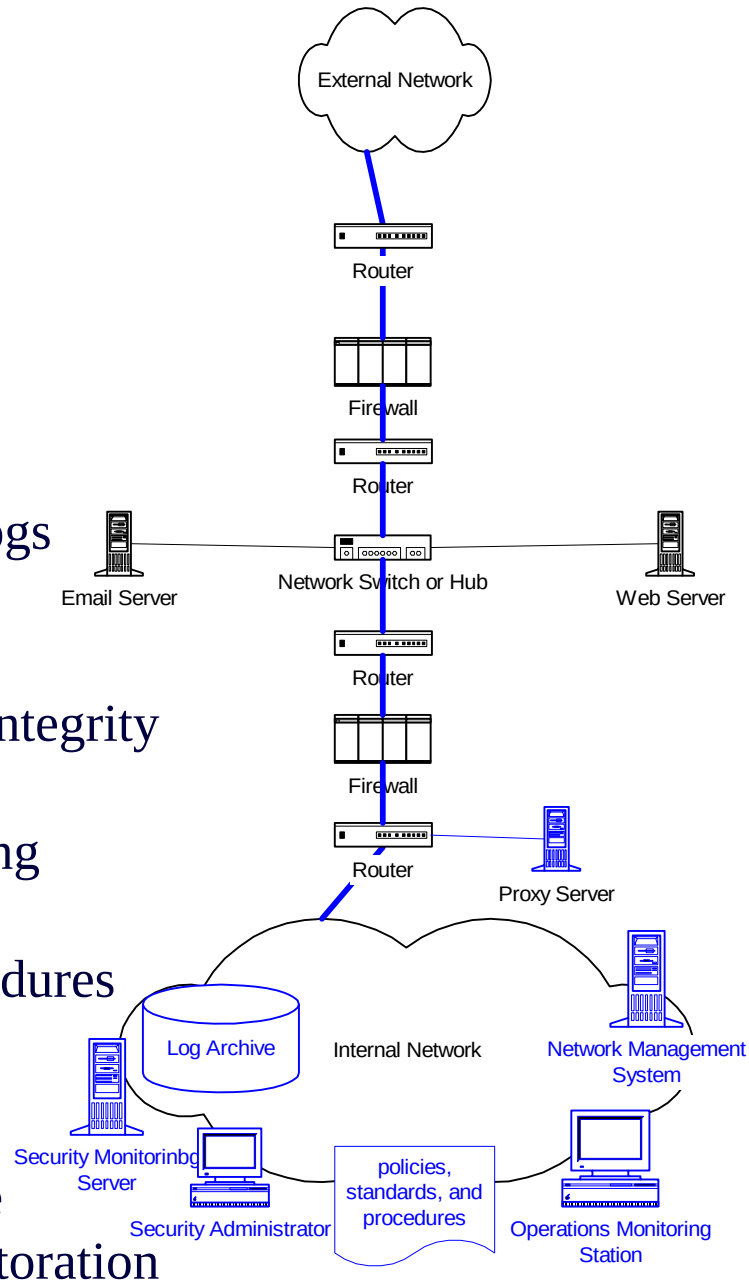
Virus or content scanners - firewalls pass certain combinations of traffic through scanner prior to allowing it to pass through, suspect data is archived

Network Intrusion Response - firewalls pass all traffic through intrusion detection systems, suspect traffic is blocked

These service brokers may be part of the firewall platform or provided by another system.

Corral Control Points

- Preventive
  - route filters
  - traffic filters
  - change control
  - identification
  - authentication
  - authorization
  - encryption
- Detective
  - network traffic logs
  - server logs
  - user activity logs
  - file and process integrity checks
  - alarms and alerting mechanisms
  - monitoring procedures
- Corrective
  - high availability
  - incident response
  - configuration restoration
  - login revocation



Prevention Controls (access)

Relevant access controls:

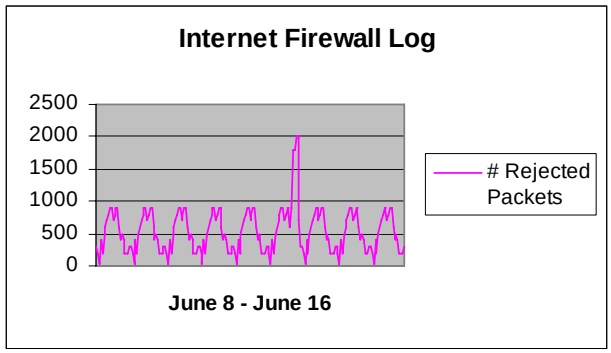
- Routers
- Firewalls
- Servers
- User Administration Systems
- Admin Administration Systems
- Network Management Systems

Prevention Controls (rules)

RULE	SOURCE	SOURCE IP	DESTINATION	DEST IP	SERVICES	PROTOCOL	PORT	ACTION	TRACK
---	---	---	---	---	---	---	---	---	---
1	Any	-	mailserver	209.134.231.68	smtp	tcp	23	accept	-
---	---	---	---	---	---	---	---	---	---
2	mailserver	209.134.231.68	Any	-	smtp	tcp	23	accept	-
---	---	---	---	---	---	---	---	---	---
3	appserver	209.134.28.2	backendsys1	171.36.14.90	appprotocol	tcp	5620	accept	-
			backendsys2	171.36.23.71					
---	---	---	---	---	---	---	---	---	---
4	Any	-	webserver	209.134.28.1	http	tcp	80	accept	-
					https	tcp	443		
---	---	---	---	---	---	---	---	---	---
5	networkmgr	171.36.142.69	webserver	209.134.28.1	ssh	tcp	22	accept	Long
	securitymgr	171.36.141.69	appserver	209.134.28.2					
---	---	---	---	---	---	---	---	---	---
6	managementconsole	171.36.48.172	Any	-	mgmtprotocol	tcp	3340	accept	-
---	---	---	---	---	---	---	---	---	---
7	Any	-	Any	-	Any	-	-	drop	Long

Detection Controls (logs)

- Patterns



- Violations

  10:10:33 accept fw1 >le1 src: admin.server dst: ecomweb.server port: 23 s_port: 4008

- Transactions

```
Tue Dec  5 15:37:10 2002 rule-editor jdoe@host7: Installing rulebase '/opt/CKPfw/conf/fw1.W' on host 'fw1'
```

- Changes

  To: Security Monitor

  Subject: Config Change on Firewall XYZ

Firewalls:

Designing a Secure Environment

EXAMPLE: CISCO PIX

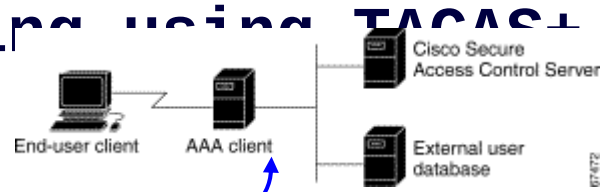
JLB, October 2002

PIX Firewall configuration components:

Firewall – performs traffic inspection, traffic filtering, network address translations (NAT)

Cisco Secure Policy Manager – allows an administrator to update a firewall configuration with a GUI

Cisco Access Control Server – performs authentication, authorization, and accounting using TACAS+ or RADIUS



From Cisco web site

PIX configuration files

The PIX config is a series of commands that are understood by the PIX. As it boots, it will read the config in its default location. It will also read a config from a floppy if inserted at boot time.

In addition, the Cisco Secure Policy manager can be configured with a “Prologue” and “Epilogue.” Each is a set of PIX commands that will be read into the PIX before and after (respectively) a config is loaded from the Policy Manager.

Most auditors work with the administrator to collect the prologue and epilogue from the Policy Manager, then dump the config directly from the firewall via telnet or ssh to an ascii file for offline analysis.

Example PIX config:

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 INTERFACE-slot:2 security10
nameif ethernet3 INTERFACE-slot:3 security20
nameif ethernet4 INTERFACE-slot:4 security30
nameif ethernet5 failover:5 security40
enable password 582gkN.qdCv6fW5 encrypted
passwd d1F2334dRN6ZME encrypted
hostname pix1
fixup protocol smtp 25
fixup protocol ftp 21
no names
access-list NETMANAGE:5 permit icmp any any echo-reply
access-list NETMANAGE :5 deny ip any any
...
access-list CLIENT permit tcp host 199.26.16.24 host 209.34.202.55 eq ftp
access-list CLIENT permit tcp host 199.26.16.24 host 209.34.203.45 eq ftp
…
logging host inside 209.34.123.200
logging host inside 209.34.123.100
...
access-group CLIENT in interface outside
access-group NETMANAGE in interface inside
…
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ (inside) host 208.34.15.131 <clear text passwd> timeout 5
aaa-server TACACS+ (inside) host 208.34.15.3 <clear text passwd> timeout 5
aaa-server RADIUS protocol radius
aaa authentication telnet console TACACS+
snmp-server host inside 208.34.14.142
snmp-server host inside 208.34.14.143
snmp-server host inside 208.34.14.26
snmp-server location New York
snmp-server contact Operations, (800) 555-1212
snmp-server community <clear text string>
snmp-server enable traps
tftp-server inside 208.34.15.134 pix1.cfg
no floodguard enable
no sysopt route dnat
isakmp identity hostname
telnet 208.34.15.0 255.255.255.0 inside
telnet 208.34.14.0 255.255.255.0 inside
telnet 208.34.15.130 255.255.255.255 inside
telnet timeout 5
ssh timeout 5
terminal width 80
```

Documentation for analyzing PIX configs:

www.cisco.com
-> Technical Documents
-> Dropdown Network Security Menu, select “Firewall”
-> Firewall OS Software
-> version
-> “Configuration Guide”

PIX logs of interest:

AAA log - shows who logged into firewall and when, but not who logged into CSPM

Individual firewall logs - where firewall has been configured for logging, traffic log will be sent to a syslog server. If the syslog server is down, the logs will be lost. Unfortunately, security logs cannot automatically be separated from performance logs, so these logs are unwieldy. Numbered messages in logs are documented at:

http://www.cisco.com/univercd/cc/td/doc/product/iabu/pix/pix_60/syslog/pixemsgs.htm

version

Ex. PIX log:

RAW, IF AVAILABLE, ALSO INCLUDES ALL NON SECURITY EVENTS:

Sep 13 01:54:08 pix1 Sep 12 2002 22:06:40: %PIX-6-302001: Built inbound TCP connection 149852855 for faddr 101.12.227.49/64474 gaddr 209.34.102.13/8204 laddr 209.34.102.13/8204

Sep 13 01:54:08 pix1 Sep 12 2002 22:07:06: %PIX-6-106015: Deny TCP (no connection) from 101.12.227.49/80 to 209.34.123.102/4483 flags ACK on interface outside

Sep 13 01:54:08 pix1 Sep 12 2002 22:06:40: %PIX-6-302001: Built inbound TCP connection 149852856 for faddr 208.34.225.104/42371 gaddr 209.34.102.13/8204 laddr 209.34.102.13/8204

Sep 13 01:54:08 pix1 Sep 12 2002 22:06:40: %PIX-6-302002: Teardown TCP connection 149852853 faddr 208.34.225.103/42625 gaddr 209.34.102.13/8204 laddr 209.34.102.13/8204 duration 0:00:01 bytes 1214 (TCP FINs)

Sep 13 01:54:08 pix1 Sep 12 2002 22:06:40: %PIX-6-302001: Built inbound TCP connection 149852857 for faddr 10.23.116.64/35411 gaddr 209.34.102.13/8204 laddr 209.34.102.13/8204

Sep 13 01:54:08 pix1 Sep 12 2002 22:06:52: %PIX-4-106023: Deny udp src outside:209.34.123.1/55337 dst DMZ-slot:2:209.34.53.163/514 by access-group " CSMInterrface "

Sep 13 01:54:08 pix1 Sep 12 2002 22:06:52: %PIX-4-106023: Deny udp src outside: 209.34.123.1/50613 dst DMZ-slot:2:209.34.53.164/514 by access-group ”CSMInterface"

PARSE, FILTER, NO GUI AVAILABLE:

TIME:	EMSGCODE:	ACTION:	PROTOCOL:	SOURCE:	S_PORT:	DESTINATION:	D_PORT:
00:55:39	%PIX-4-106023	Deny	udp	10.23.248.13	50000	208.34.225.83	53
00:56:02	%PIX-6-106015	Deny	TCP	208.34.227.49	80	208.34.129.102	1653
00:56:02	%PIX-6-106015	Deny	TCP	208.34.227.49	80	208.34.129.102	1653

TIME: the time of the event

EMSGCODE: the system log message number that specifies the meaning of the message

ACTION: what the firewall did with the session

PROTOCOL: the type of network traffic

SOURCE: the IP or host name of the source

SPORT: the port on the source machine from which it initiated the traffic

DESTINATION: the IP or host name of the destination

DPORT: the port on the destination machine on which it received the traffic

Firewalls:

Designing a Secure Environment

EXAMPLE: CHECKPOINT FireWall-1

JLB, October 2002

Checkpoint Firewall configuration components:

Firewall – performs traffic inspection, traffic filtering, network address translations (NAT), administrator access control and logging

Firewall Management Station – allows an administrator to update multiple firewalls with a single GUI, is required for user-level authentication and authorization features

Checkpoint config files

In the checkpoint install directory, /var/opt/CHKPfw (or something equilavent) all config files reside. Most significant are:

- objects.C - combined object file for all firewalls managed by this install
- <individual firewall name>.W - rules for individual firewall
- <individual firewall name>.pf - compiled version of rules combined with IPs found in object.C file at compile time
- fwauth.NDB - database of authorized users and administrators
- gui-clients - IPs of administrator workstations

Most auditors work with the administrator to view users through online utilities and take the ".W" and ".C" files offline to audit rules. They are easy to read and scripts are available to parse them into spreadsheet and HTML format.

Example Checkpoint Object:

objects.C - host, network, and service definitions

```
: (host7
                        :type (host)
                        :read_community (public)
                        :write_community (private)
                        :show_in_menus (true)
                        :netobj_adtr_method (adtr_static)
                        :ipaddr (209.34.123.46)
                        :comments (“user workstation 23532”)
                        :info ()
                        :location (internal)
                        :firewall (”fw1")
                        :color (Blue)
                        :vendor_info ()
                        :host_schemes_val (51)
                        :host_schemes_names (
                                : ("S/Key")
                                : (SecurID)
                                : (RADIUS)
                                : (Defender)
                        )
                        :add_adtr_rule (false)
                        :valid_ipaddr ()
                        :external_interface ()
                        :embedded_lictype (50
                                :num (50)
                        )
                )
```

Example Checkpoint Rule:

<firewallname>.W - firewall and NAT rule definitions

```
rule (
                :src (
                        : host7
                )
                :dst (
                        : clienthost1
                )
                :services (
                        : ssh
                )
                :action (
                        : (accept
                                :type (accept)
                                :color ("Dark green")
                                :macro (RECORD_CONN)
                                :icon-name (icon-accept)
                                :text-rid (61463)
                                :windows-color (green)
                        )
                )
                :track (
                        : Long
                )
                :install (
                        : fw1
                )
                :time (
                        : Any
                )
                :comments (“Project ID 52671”)
        )
```

Documentation for analyzing Checkpoint configs:

www.checkpoint.com
online docs and parsing scripts available, but password protected, need to get password from holder of maintenance contract

Checkpoint logs of interest:

UI log - shows who logged in when and what actions were performed, if Firewall is managed on a server, it will reside on the server and it will not be possible to administer the firewall locally

Individual firewall logs - where rule have been tagged for logging, traffic log will be stored on individual firewall or sent to mgmt server. If mgmt server is down, buffer is kept on individual firewall. The last “Drop All” rule SHOULD be tagged for “long” logging.

Ex. Checkpoint log:

RAW:

```
3;13Sep2002;21:40:56;fw1;log;drop;;exte;inbound;udp;135.18.25.1; 209.34.123.1;ntp;ntp;;25;;;;76;;;;;
4;13Sep2002;21:41:17;fw1;log;drop;;exte;inbound;udp;130.12.219.1; 209.34.123.2;ntp;ntp;;25;;;;76;;;;;
```

PARSE OR VIEW VIA GUI:

TIME:	RULE:	I/F:	ACTION:	SOURCE:	DESTINATION:	PROTOCOL :	SERVICE:	SRCPORT:
21:50:29	25	exte	drop	15.16.219.2	209.44.123.11	udp	ntp	ntp
21:50:46	25	exte	drop	209.34.123.15	209.44.123.11	udp	ntp	ntp
21:51:15	2	int	accept	209.34.123.65	204.10.23.6	tcp	ftp	41333
21:51:17	2	int	accept	209.34.123.9	108.203.10.8	tcp	ftp	2048
21:51:19	2	exte	accept	137.17.147.9	209.44.123.8	tcp	2099	2099

TIME: the time of the event

RULE: the rule number on the firewall which triggered the log (no such feature as yet on PIX)

I/F: the network interface on which the rule was triggered

ACTION: what the firewall did with the session

SOURCE: the IP or host name of the source

DESTINATION: the IP or host name of the destination

PROTOCOL: the type of network traffic

SERVICE: either a predefined service definition or the protocol/port definition of the service

SRC PORT: the port on the source machine from which it initiated the traffic

ADMIN INTERFACE LOG:

```
Tue Dec  5 16:15:01 2002 rule-editor jdoe@host7: Locking DB with '01010101' permissions
Tue Dec  5 16:17:18 2002 rule-editor jdoe@host7: Locking DB with '01010101' permissions
Tue Dec  5 16:17:42 2002 rule-editor jdoe@host7: Storing objects
Tue Dec  5 16:17:42 2002 rule-editor jdoe@host7: Storing rulebase(s)
Tue Dec  5 16:17:42 2002 rule-editor jdoe@host7: Storing rulebase 'default.W'
Tue Dec  5 16:17:42 2002 rule-editor jdoe@host7: Storing rulebase 'safe.W'
Tue Dec  5 16:17:42 2002 rule-editor jdoe@host7: Storing rulebase 'wafw.W'
```

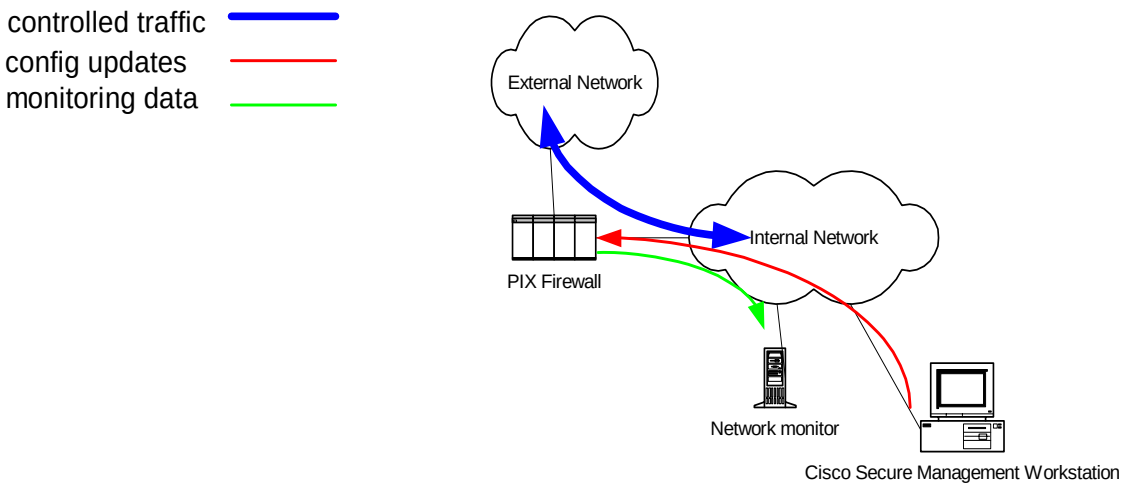
Firewalls:

Designing a Secure Environment

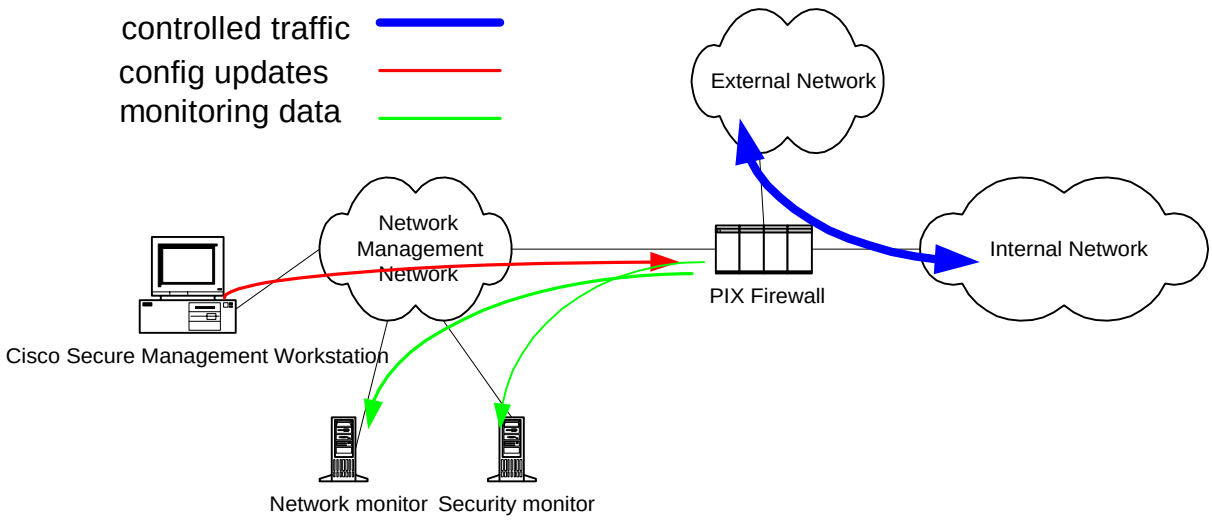
DESIGN ALTERNATIVES

JLB, October 2002

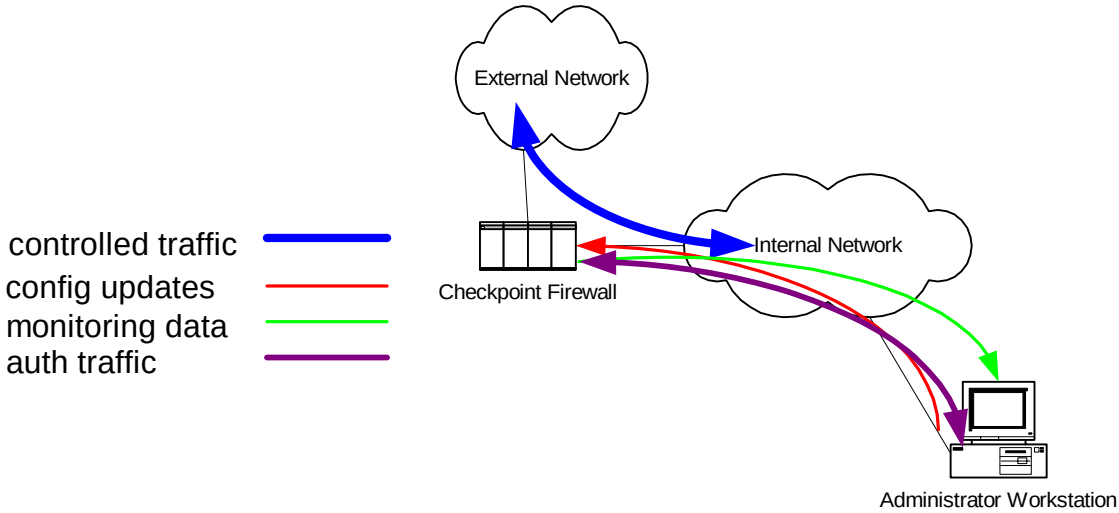
Comparison PIX Firewall configuration:



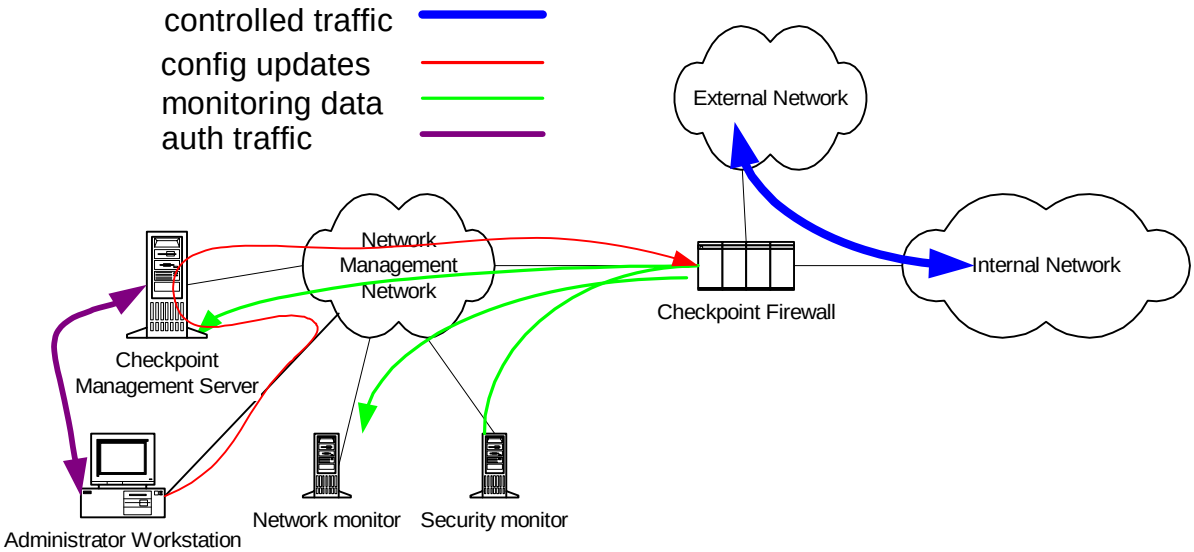
Preferred:



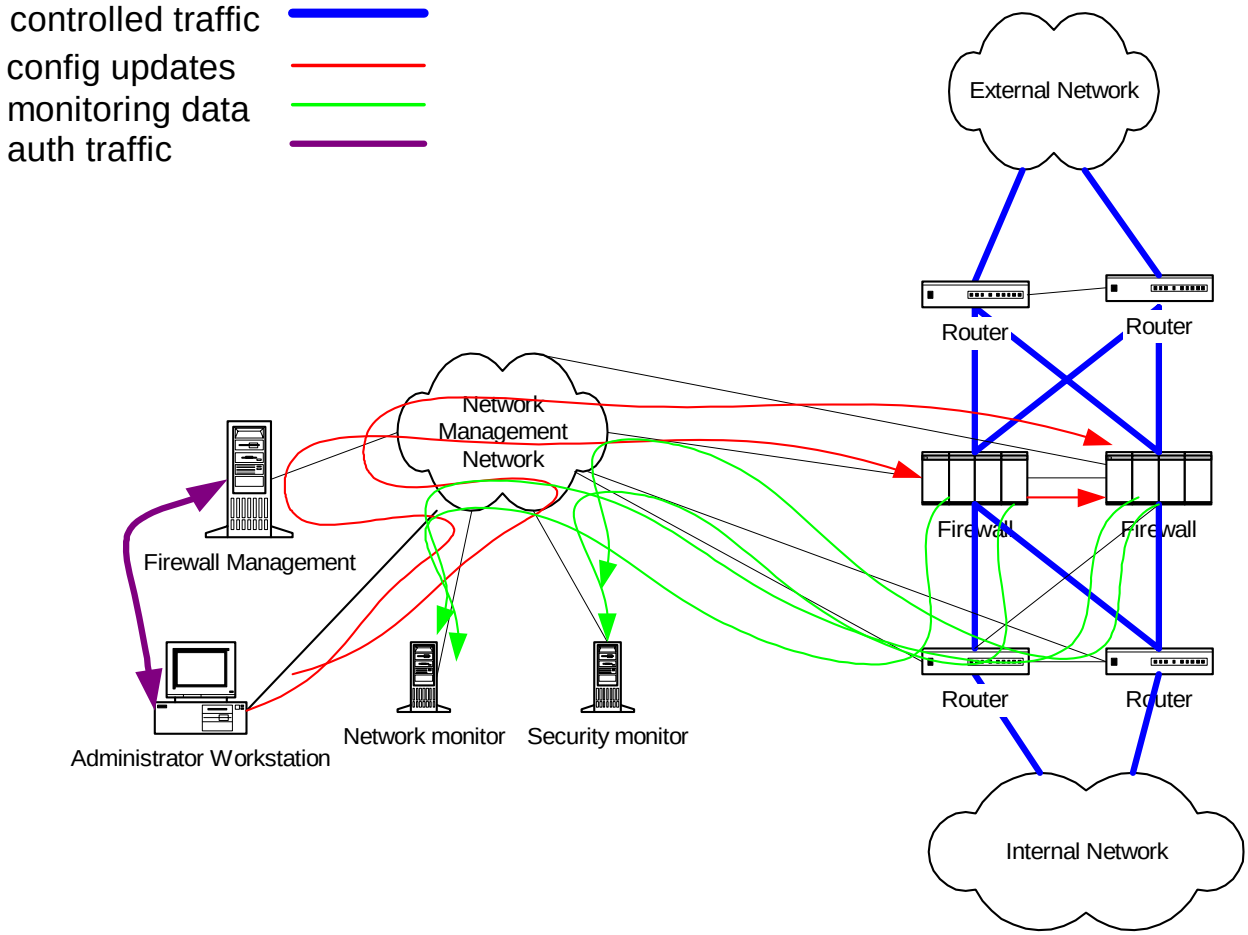
Comparison Checkpoint Firewall configuration:



Preferred:



High Availability



Quick Design Tips

Inbound

- Only when hosting a Network Site
- Open the minimum number of IPs and ports, one way in

Outbound

- NAT users behind single access point
- Open the minimum number of ports, one way out

Both

- Firewall should default to deny
- If service brokers are down, firewall should still run
- Only open rule for support systems that are very secure
- Never open for future use

Firewalls:

Designing a Secure Environment

October 14, 2002

Jennifer L. Bayuk
Bear Stearns & Co., Inc
jbayuk@bear.com