



Firewall Configuration

Firewall name: acmecorp-pix

Firewall model: CiscoPIX

Completed on Thu Jul 15 11:51:46 CDT 2010

config.txt

```
1 acmecorp-pix# show config
2 : Saved
3 : Written by enable_15 at 15:55:14.799 UTC Wed Mar 29 2006
4 PIX Version 6.3(3)
5 interface ethernet0 auto
6 interface ethernet1 100basetx
7 interface ethernet2 auto
8 interface ethernet3 auto
9 interface ethernet4 auto
10 interface ethernet5 auto shutdown
11 nameif ethernet0 outside security0
12 nameif ethernet1 inside security100
13 nameif ethernet2 mail1 security50
14 nameif ethernet3 testweb security10
15 nameif ethernet4 proxymail security20
16 nameif ethernet5 vpn4 security80
17 enable password ***** encrypted
18 passwd ***** encrypted
19 hostname acmecorp-pix
20 domain-name acmecorp.com
21 fixup protocol dns maximum-length 512
22 fixup protocol ftp 21
23 fixup protocol h323 h225 1720
24 fixup protocol h323 ras 1718-1719
25 fixup protocol http 80
26 fixup protocol rsh 514
27 fixup protocol rtsp 554
28 fixup protocol sip 5060
29 fixup protocol sip udp 5060
30 fixup protocol skinny 2000
31 fixup protocol smtp 25
32 fixup protocol sqlnet 1521
33 fixup protocol tftp 69
34 names
35 object-group service web_svcs tcp
36 port-object eq www
37 port-object eq https
38 object-group service mail_svcs tcp
39 port-object eq smtp
40 port-object eq pop3
41 object-group service inet_svcs tcp
42 port-object eq smtp
43 port-object eq pop3
```

44 port-object eq www
45 port-object eq https
46 port-object eq domain
47 object-group service common_ports tcp
48 port-object eq ssh
49 port-object eq telnet
50 group-object web_svcs
51 group-object inet_svcs
52 object-group network db_svcs
53 network-object host 172.16.1.200
54 network-object host 172.16.1.210
55 object-group network internal_mail_svcs
56 network-object host 172.16.2.200
57 network-object host 172.16.2.210
58 access-list acl_outside permit tcp any host 62.59.14.161 eq www
59 access-list acl_outside permit tcp any host 62.59.14.161 eq https
60 access-list acl_outside permit tcp 216.74.18.32 255.255.255.224 host 62.59.14.163 eq smtp
61 access-list acl_outside permit tcp host 207.135.79.64 host 62.59.14.169 eq 9595
62 access-list acl_outside permit tcp 207.38.18.128 255.255.255.224 host 62.59.14.163 eq smtp
63 access-list acl_outside permit tcp any host 62.59.14.170 eq www
64 access-list acl_outside permit tcp any host 62.59.14.171 eq www
65 access-list acl_outside permit tcp any host 62.59.14.171 eq https
66 access-list acl_outside permit tcp any host 62.59.14.171 eq ssh
67 access-list acl_outside permit tcp host 69.237.83.3 host 62.59.14.171 eq 7777
68 access-list acl_outside permit tcp 66.179.26.128 255.255.255.192 host 62.59.14.163 eq smtp
69 access-list acl_outside permit tcp 66.179.109.160 255.255.255.224 host 62.59.14.163 eq smtp
70 access-list acl_outside permit tcp 216.183.119.96 255.255.255.224 host 62.59.14.163 eq smtp
71 access-list acl_outside permit tcp 64.92.205.64 255.255.255.224 host 62.59.14.163 eq smtp
72 access-list acl_outside permit tcp 208.65.144.0 255.255.248.0 host 62.59.14.163 eq smtp
73 access-list acl_outside permit icmp any host 62.59.14.169
74 access-list acl_outside permit tcp any host 62.59.14.169 eq https
75 access-list acl_outside permit tcp any host 62.59.14.169 eq 8080
76 access-list acl_outside permit tcp any host 62.59.14.169 object-group web_svcs
77 access-list acl_outside permit tcp any host 62.59.14.200 eq www
78 access-list acl_outside permit tcp any host 62.59.14.200 eq https
79 access-list acl_mail1 permit tcp any host 192.168.1.4 eq smtp
80 access-list acl_mail1 permit tcp any host 192.168.1.2 eq smtp
81 access-list acl_mail1 permit tcp any host 192.168.1.2 eq pop3
82 access-list acl_mail1 permit udp host 192.168.1.2 any eq domain
83 access-list acl_mail1 deny tcp any host 192.168.1.2 object-group mail_svcs
84 access-list acl_mail1 permit tcp host 192.168.1.200 object-group db_svcs eq 118
85 access-list acl_mail1 permit udp host 192.168.1.200 object-group db_svcs eq 118
86 access-list acl_inside permit tcp any any eq www
87 access-list acl_inside permit tcp any any eq https
88 access-list acl_inside permit tcp any any eq 5405
89 access-list acl_inside permit tcp host 172.16.0.24 any eq ftp
90 access-list acl_inside permit tcp host 172.16.0.24 any eq ssh
91 access-list acl_inside permit tcp any any eq ftp
92 access-list acl_inside permit tcp any any eq ssh
93 access-list acl_inside permit tcp any any eq 81
94 access-list acl_inside permit tcp any any eq telnet
95 access-list acl_inside permit udp host 172.16.0.68 any eq domain
96 access-list acl_inside permit tcp any any eq 9895
97 access-list acl_inside permit tcp any any eq nntp
98 access-list acl_inside permit udp host 172.16.0.68 any eq ntp
99 access-list acl_inside permit tcp host 172.16.0.25 any eq 2847
100 access-list acl_inside permit tcp host 172.16.0.25 any eq 2848
101 access-list acl_inside permit tcp any any eq 7618
102 access-list acl_inside permit tcp any any eq 8080
103 access-list acl_inside permit tcp host 172.16.0.19 any eq smtp
104 access-list acl_inside permit tcp host 172.16.0.19 any eq ftp
105 access-list acl_inside permit tcp host 172.16.0.19 any eq ssh

106 access-list acl_inside permit icmp any any
107 access-list acl_inside permit tcp any any eq h323
108 access-list acl_inside permit udp any any
109 access-list acl_inside permit udp host 192.168.5.251 any
110 access-list acl_inside permit tcp any any eq 5900
111 access-list acl_inside permit udp host 192.168.5.250 any
112 access-list acl_inside permit tcp any host 192.168.50.2 eq 5901
113 access-list acl_inside permit tcp any any eq 5901
114 access-list acl_inside permit udp any any eq 5901
115 access-list acl_inside deny tcp 172.16.0.0 255.255.0.0 any range 1024 65535
116 access-list acl_inside deny udp any any range 135 139
117 access-list acl_inside permit udp any host 172.16.0.4 eq ntp
118 access-list acl_inside permit tcp 172.16.0.0 255.255.0.0 any eq nntp
119 access-list acl_inside permit tcp any any eq 7777
120 access-list acl_inside permit tcp host 172.16.0.15 any eq ftp
121 access-list acl_inside permit tcp host 172.16.0.15 any eq ssh
122 access-list acl_guest permit tcp any any eq www
123 access-list acl_guest permit tcp any any eq ftp
124 access-list acl_guest permit tcp any any eq pop3
125 access-list acl_guest permit udp any any eq domain
126 access-list acl_guest permit tcp any any eq smtp
127 access-list acl_guest permit icmp any any
128 access-list acl_guest permit udp any any
129 access-list acl_guest permit tcp any any
130 access-list 110 permit ip 172.16.0.0 255.255.0.0 192.168.16.0 255.255.255.0
131 access-list 110 permit ip 10.0.0.0 255.0.0.0 192.168.16.0 255.255.255.0
132 access-list acl_testweb permit tcp any any eq www
133 access-list acl_testweb permit tcp any any eq https
134 access-list acl_testweb permit tcp any any eq ssh
135 access-list acl_testweb permit tcp any any eq smtp
136 access-list acl_testweb permit udp any any eq dnsix
137 access-list acl_testweb permit icmp any any
138 access-list acl_testweb permit udp any any eq domain
139 access-list acl_proxymail permit tcp any any object-group web_svcs
140 access-list acl_proxymail permit tcp any any object-group mail_svcs
141 access-list acl_proxymail permit tcp any any object-group inet_svcs
142 access-list acl_proxymail permit icmp any any
143 pager lines 25
144 logging on
145 logging buffered debugging
146 logging trap informational
147 logging host inside 172.16.0.200
148 mtu outside 1500
149 mtu inside 1500
150 mtu mail1 1500
151 mtu testweb 1500
152 mtu proxymail 1500
153 mtu vpn4 1500
154 ip address outside 62.59.14.189 255.255.255.224
155 ip address inside 172.16.0.1 255.255.0.0
156 ip address mail1 192.168.1.1 255.255.255.0
157 ip address testweb 192.168.50.1 255.255.255.0
158 ip address proxymail 192.168.9.1 255.255.255.0
159 ip address vpn4 127.0.0.1 255.255.255.255
160 ip audit info action alarm
161 ip audit attack action alarm
162 ip local pool ippool 192.168.16.2-192.168.16.50
163 no failover
164 failover timeout 0:00:00
165 failover poll 15
166 no failover ip address outside
167 no failover ip address inside

168 no failover ip address mail1
169 no failover ip address testweb
170 no failover ip address proxymail
171 no failover ip address vpn4
172 pdm location 10.0.0.0 255.0.0.0 inside
173 pdm location 172.16.0.24 255.255.255.255 inside
174 pdm location 172.16.6.44 255.255.255.255 inside
175 pdm location 172.16.31.46 255.255.255.255 inside
176 pdm location 192.168.0.0 255.255.255.0 inside
177 pdm location 192.168.1.2 255.255.255.255 mail1
178 pdm location 172.16.0.2 255.255.255.255 inside
179 pdm location 172.16.0.3 255.255.255.255 inside
180 pdm location 172.16.0.101 255.255.255.255 inside
181 pdm location 172.16.6.21 255.255.255.255 inside
182 pdm location 192.168.2.0 255.255.255.0 inside
183 pdm location 192.168.3.0 255.255.255.0 inside
184 pdm location 192.168.4.0 255.255.255.0 inside
185 pdm location 192.168.5.0 255.255.255.0 inside
186 pdm location 172.16.0.57 255.255.255.255 inside
187 pdm location 172.16.0.200 255.255.255.255 inside
188 pdm history enable
189 arp timeout 14400
190 global (outside) 2 62.59.14.163
191 global (outside) 3 62.59.14.164
192 global (outside) 4 62.59.14.165
193 global (outside) 5 62.59.14.166
194 global (outside) 6 62.59.14.167
195 global (outside) 7 62.59.14.168
196 global (outside) 1 62.59.14.162
197 global (mail1) 1 192.168.1.3
198 global (testweb) 1 192.168.50.3
199 global (testweb) 3 192.168.50.4
200 global (testweb) 6 192.168.50.5
201 global (testweb) 7 192.168.50.6
202 nat (inside) 0 access-list 110
203 nat (inside) 6 192.168.2.0 255.255.255.0 0 0
204 nat (inside) 3 192.168.3.0 255.255.255.0 0 0
205 nat (inside) 4 192.168.4.0 255.255.255.0 0 0
206 nat (inside) 5 192.168.5.0 255.255.255.0 0 0
207 nat (inside) 1 172.16.0.0 255.255.0.0 0 0
208 nat (inside) 7 172.17.0.0 255.255.0.0 0 0
209 nat (inside) 7 10.0.0.0 255.0.0.0 0 0
210 nat (mail1) 1 0.0.0.0 0.0.0.0 0 0
211 nat (testweb) 1 0.0.0.0 0.0.0.0 0 0
212 static (inside,outside) 62.59.14.163 172.16.1.201 netmask 255.255.255.255 0 0
213 static (mail1,outside) 62.59.14.200 192.168.1.200 netmask 255.255.255.255 0 0
214 static (inside,mail1) 192.168.1.4 172.16.0.19 netmask 255.255.255.255 0 0
215 static (inside,mail1) 172.16.1.200 172.168.1.200 netmask 255.255.255.255 0 0
216 static (inside,mail1) 172.16.1.210 172.168.1.210 netmask 255.255.255.255 0 0
217 static (testweb,outside) 62.59.14.171 192.168.50.2 netmask 255.255.255.255 0 0
218 static (proxymail,outside) 62.59.14.169 192.168.9.2 netmask 255.255.255.255 0 0
219 static (proxymail,outside) 62.59.14.161 192.168.9.2 netmask 255.255.255.255 0 0
220 access-group acl_outside in interface outside
221 access-group acl_inside in interface inside
222 access-group acl_mail1 in interface mail1
223 access-group acl_testweb in interface testweb
224 access-group acl_proxymail in interface proxymail
225 route outside 0.0.0.0 0.0.0.0 62.59.14.190 1
226 route inside 10.0.0.0 255.0.0.0 172.16.0.51 1
227 route inside 172.17.0.0 255.255.0.0 172.16.0.51 1
228 route inside 192.168.2.0 255.255.255.0 172.16.0.51 1
229 route inside 192.168.3.0 255.255.255.0 172.16.0.51 1

```

230 route inside 192.168.4.0 255.255.255.0 172.16.0.51 1
231 route inside 192.168.5.0 255.255.255.0 172.16.0.51 1
232 timeout xlate 1:00:00
233 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
234 timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
235 timeout uauth 0:05:00 absolute
236 aaa-server TACACS+ protocol tacacs+
237 aaa-server RADIUS protocol radius
238 aaa-server LOCAL protocol local
239 aaa-server partnerauth protocol radius
240 aaa-server partnerauth (inside) host 172.16.0.25 PHASE2 timeout 5
241 http server enable
242 http 172.16.31.46 255.255.255.255 inside
243 http 172.16.6.44 255.255.255.255 inside
244 http 172.16.0.101 255.255.255.255 inside
245 http 172.16.0.200 255.255.255.255 inside
246 snmp-server host inside 172.16.0.61
247 snmp-server location San Jose PIX
248 snmp-server contact AcmeCorp
249 snmp-server community harry
250 snmp-server enable traps
251 floodguard enable
252 sysopt connection permit-ipsec
253 crypto ipsec transform-set sjset esp-3des esp-sha-hmac
254 crypto dynamic-map dynmap 10 set transform-set sjset
255 crypto map sjmap 10 ipsec-isakmp dynamic dynmap
256 crypto map sjmap client authentication partnerauth
257 crypto map sjmap interface outside
258 isakmp enable outside
259 isakmp identity address
260 isakmp policy 10 authentication pre-share
261 isakmp policy 10 encryption des
262 isakmp policy 10 hash md5
263 isakmp policy 10 group 2
264 isakmp policy 10 lifetime 86400
265 vpngroup remotesj04 address-pool ippool
266 vpngroup remotesj04 dns-server 172.16.0.3
267 vpngroup remotesj04 wins-server 172.16.0.25
268 vpngroup remotesj04 default-domain acmecorp.com
269 vpngroup remotesj04 split-tunnel 110
270 vpngroup remotesj04 idle-time 1800
271 vpngroup remotesj04 password *****
272 telnet 172.16.0.0 255.255.0.0 inside
273 telnet 192.168.3.0 255.255.255.0 inside
274 telnet timeout 60
275 ssh timeout 5
276 console timeout 0
277 terminal width 80
278 banner motd WARNING: Unauthorized access to this device will result in prosecution to the fullest extent
permissible by law
279 Cryptochecksum:74151f0b71a7d641d691819297fc6c74

```

route.txt

```

1 acmecorp-pix# show route
2 outside 62.59.14.189 255.255.255.224 62.59.14.189 1 CONNECT static
3 inside 172.16.0.0 255.255.0.0 172.16.0.1 1 CONNECT static
4 mail1 192.168.1.0 255.255.255.0 192.168.1.1 1 CONNECT static
5 testweb 192.168.50.0 255.255.255.0 192.168.50.1 1 CONNECT static
6 proxymail 192.168.9.0 255.255.255.0 192.168.9.1 1 CONNECT static
7 outside 0.0.0.0 0.0.0.0 62.59.14.190 1 CONNECT static

```

8 inside 10.0.0.0 255.0.0.0 172.16.0.51 1 CONNECT static
9 inside 172.17.0.0 255.255.0.0 172.16.0.51 1 CONNECT static
10 inside 192.168.2.0 255.255.255.0 172.16.0.51 1 CONNECT static
11 inside 192.168.3.0 255.255.255.0 172.16.0.51 1 CONNECT static
12 inside 192.168.4.0 255.255.255.0 172.16.0.51 1 CONNECT static
13 inside 192.168.5.0 255.255.255.0 172.16.0.51 1 CONNECT static