

Firewall Cleanup and Optimization

Firewall name: acmecorp-pix

Firewall model: CiscoPIX

Completed on Thu Jul 15 11:27:18 CDT 2010

This report provides an analysis of the firewall ACL rules based on rule relationships and rule usage obtained from access list hit count output. It identifies redundant, shadowed, or unused rules that are candidates for being removed from the configuration. It also identifies the most frequently used rules and recommends an optimized rule order to improve firewall analysis. The configuration changes recommended by this report will not cause any change in the behavior of the firewall.

The access list hit count output is obtained using "show access-list" command. The output contains the hit count data for each access list entry. This data is reset once a firewall is rebooted or reset explicitly using the command "clear access-list [id] counters".

Configuration Summary

We found a total of 30.7% of rules (35 of 114) that can potentially be removed from the rule base.

Explicit ACL Rules	93
Network Group Objects	2
Network Objects	0
Service Group Objects	4
Service Objects	0

Structural Rule and Object Cleanup

Redundant and Shadowed Rules	19
Unreferenced Network Objects	1
Unreferenced Service Objects	1

Usage-Based Rule and Object Cleanup

Unused Rules	28
Rule Objects Usage	
Rules with Unused Objects	0
Network Objects Usage	
Unused Network Objects	0
Network Objects with Unused Members	0
Service Objects Usage	
Unused Service Objects	0
Service Objects with Unused Members	1

Rule Optimization

Most Used Rules	57
Rule Order Dependency	4
Optimized Rule Order	

Miscellaneous Rule Attributes

Disabled Rules	0
Time Inactive Rules	0

Redundant and Shadowed Rules

This section lists all the rules that make no unique contribution to firewall behavior. Redundant rules will never match a packet because one or more preceding rules match first. These rules are indicated with the text, "Redundant to <line or rule number>". Shadowed rules are similar to redundant rules, but have an opposite action to the shadowing rule(s) and so indicate a possible error in the configuration. These rules are indicated with the text, "Shadowed by <line or rule number>". These rules may be safely disabled or removed entirely from the ruleset.

In addition, some rules are indicated as "Potentially redundant to <line or rule number>". These are rules that are a special case of a succeeding rule and may not be required. Before disabling or removing these rules, you need to examine whether there is logging, application inspection, authentication, tracking, QOS, or other options on one rule but not the other. If you remove the potentially redundant rule, you may change the behavior of any special processing resulting from such rule options. If these changes are acceptable, then you may disable or remove the redundant rule. Otherwise leave it as is. For a step-by-step process for removing these rules, please see the user manual page on [Rule Cleanup](#)

- 74 access-list acl_outside permit tcp any host 62.59.14.169 eq https**
Redundant to <76>
- 76 access-list acl_outside permit tcp any host 62.59.14.169 object-group web_svcs
- 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
- 83 access-list acl_mail1 deny tcp any host 192.168.1.2 object-group mail_svcs**
Shadowed by <80>, <81>
- 89 access-list acl_inside permit tcp host 172.16.0.24 any eq ftp**
Redundant to <91>
- 90 access-list acl_inside permit tcp host 172.16.0.24 any eq ssh**
Redundant to <92>
- 91 access-list acl_inside permit tcp any any eq ftp
- 92 access-list acl_inside permit tcp any any eq ssh
- 95 access-list acl_inside permit udp host 172.16.0.68 any eq domain**
Redundant to <108>
- 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**
Redundant to <108>
- 104 access-list acl_inside permit tcp host 172.16.0.19 any eq ftp**
Redundant to <91>
- 105 access-list acl_inside permit tcp host 172.16.0.19 any eq ssh**
Redundant to <92>
- 108 access-list acl_inside permit udp any any
- 109 access-list acl_inside permit udp host 192.168.5.251 any**
Redundant to <108>
- 111 access-list acl_inside permit udp host 192.168.5.250 any**
Redundant to <108>
- 112 access-list acl_inside permit tcp any host 192.168.50.2 eq 5901**
Redundant to <113>
- 113 access-list acl_inside permit tcp any any eq 5901
- 114 access-list acl_inside permit udp any any eq 5901**
Redundant to <108>
- 116 access-list acl_inside deny udp any any range 135 139**
Shadowed by <108>
- 117 access-list acl_inside permit udp any host 172.16.0.4 eq ntp**
Redundant to <98>, <108>
- 118 access-list acl_inside permit tcp 172.16.0.0 255.255.0.0 any eq nntp**
Redundant to <97>
- 120 access-list acl_inside permit tcp host 172.16.0.15 any eq ftp**
Redundant to <91>
- 121 access-list acl_inside permit tcp host 172.16.0.15 any eq ssh**
Redundant to <92>
- 139 access-list acl_proxymail permit tcp any any object-group web_svcs**
Redundant to <141>
- 140 access-list acl_proxymail permit tcp any any object-group mail_svcs**
Redundant to <141>

Unreferenced Network Objects

A network object is considered unused if it is not referenced by any ACL or NAT rules, either directly or indirectly through a parent or ancestor object that contains the network object as a member. These objects are candidates for removal from the configuration.

Name	Type	Members/IP Address
internal_mail_svcs	host	172.16.2.200
		172.16.2.210

Unreferenced Service Objects

A service object is considered unused if it is not referenced by any ACL or NAT rules, either directly or indirectly through a parent or ancestor object that contains the service object as a member. These objects are candidates for removal from the configuration.

Name	Type	Members/Port/Protocol
common_ports	group	inet_svcs
		web_svcs
	tcp	ssh
		telnet

Unused Rules

This section lists all the rules which have a hit count of zero in the access hit count output. These rules are candidates for removal from the configuration because they may no longer be used. This analysis is only applicable for the period since the last time access list hit counts are reset or the firewall is rebooted, so it is possible that some rules are still used but were simply not triggered during the usage period. Removing these rules will cause a change in firewall behavior.

This section also lists rules which are not applied to any interface. These rules can be removed safely.

Note that there may be some overlap between these rules and those listed in the Redundant and Shadowed Rules section because rules that made redundant by preceding rules will never be present in the access-list hit count data.

```

83 access-list acl_mail1 deny tcp any host 192.168.1.2 object-group mail_svcs
85 access-list acl_mail1 permit udp host 192.168.1.200 object-group db_svcs eq 118

88 access-list acl_inside permit tcp any any eq 5405
93 access-list acl_inside permit tcp any any eq 81
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
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
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
114 access-list acl_inside permit udp any any eq 5901
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
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

136 access-list acl_testweb permit udp any any eq dnsix

```

Rule Objects Usage

This section shows the hit counts for each rule ordered by most used to least used.

Line No	Hit Count	Source	Destination	Service	Action	ACL Name
64	56643	any (100%)	62.59.14.171 (100%)	www (100%)	accept	acl_outside
82	55321	192.168.1.2 (100%)	any (100%)	domain (100%)	accept	acl_mail1
65	54267	any (100%)	62.59.14.171 (100%)	https (100%)	accept	acl_outside
63	48845	any (100%)	62.59.14.170 (100%)	www (100%)	accept	acl_outside
59	41522	any (100%)	62.59.14.161 (100%)	https (100%)	accept	acl_outside
73	37864	any (100%)	62.59.14.169 (100%)	icmp (100%)	accept	acl_outside
62	33468	207.38.18.128/27 (100%)	62.59.14.163 (100%)	smtp (100%)	accept	acl_outside
106	26647	any (100%)	any (100%)	icmp (100%)	accept	acl_inside
60	25363	216.74.18.32/27 (100%)	62.59.14.163 (100%)	smtp (100%)	accept	acl_outside
58	23572	any (100%)	62.59.14.161 (100%)	www (100%)	accept	acl_outside
115	22461	172.16.0.0/16 (100%)	any (100%)	1024-65535 (100%)	deny	acl_inside
81	13255	any (100%)	192.168.1.2 (100%)	pop3 (100%)	accept	acl_mail1
137	12674	any (100%)	any (100%)	icmp (100%)	accept	acl_testweb
142	11645	any (100%)	any (100%)	icmp (100%)	accept	acl_proxymail
76	11543	any (100%)	62.59.14.169 (100%)	web_svcs (100%)	accept	acl_outside
74	9736	any (100%)	62.59.14.169 (100%)	https (100%)	accept	acl_outside
138	8935	any (100%)	any (100%)	domain (100%)	accept	acl_testweb
108	8893	any (100%)	any (100%)	udp (100%)	accept	acl_inside
103	8857	172.16.0.19 (100%)	any (100%)	smtp (100%)	accept	acl_inside
84	8847	192.168.1.200 (100%)	db_svcs (100%)	118 (100%)	accept	acl_mail1
98	7984	172.16.0.68 (100%)	any (100%)	ntp (100%)	accept	acl_inside
79	7784	any (100%)	192.168.1.4 (100%)	smtp (100%)	accept	acl_mail1

Line No	Hit Count	Source	Destination	Service	Action	ACL Name
91	7534	any (100%)	any (100%)	ftp (100%)	accept	acl_inside
80	7445	any (100%)	192.168.1.2 (100%)	smtp (100%)	accept	acl_mail1
139	7009	any (100%)	any (100%)	web_svcs (100%)	accept	acl_proxymail
102	6846	any (100%)	any (100%)	8080 (100%)	accept	acl_inside
87	6684	any (100%)	any (100%)	https (100%)	accept	acl_inside
135	5578	any (100%)	any (100%)	smtp (100%)	accept	acl_testweb
141	4794	any (100%)	any (100%)	inet_svcs (100%)	accept	acl_proxymail
75	4423	any (100%)	62.59.14.169 (100%)	8080 (100%)	accept	acl_outside
86	3654	any (100%)	any (100%)	www (100%)	accept	acl_inside
66	2253	any (100%)	62.59.14.171 (100%)	ssh (100%)	accept	acl_outside
140	1723	any (100%)	any (100%)	mail_svcs (100%)	accept	acl_proxymail
133	1255	any (100%)	any (100%)	https (100%)	accept	acl_testweb
61	1254	207.135.79.64 (100%)	62.59.14.169 (100%)	9595 (100%)	accept	acl_outside
132	1212	any (100%)	any (100%)	www (100%)	accept	acl_testweb
68	854	66.179.26.128/26 (100%)	62.59.14.163 (100%)	smtp (100%)	accept	acl_outside
70	698	216.183.119.96/27 (100%)	62.59.14.163 (100%)	smtp (100%)	accept	acl_outside
92	645	any (100%)	any (100%)	ssh (100%)	accept	acl_inside
69	576	66.179.109.160/27 (100%)	62.59.14.163 (100%)	smtp (100%)	accept	acl_outside
99	574	172.16.0.25 (100%)	any (100%)	2847 (100%)	accept	acl_inside
112	475	any (100%)	192.168.50.2 (100%)	5901 (100%)	accept	acl_inside
90	462	172.16.0.24 (100%)	any (100%)	ssh (100%)	accept	acl_inside
72	426	208.65.144.0/21 (100%)	62.59.14.163 (100%)	smtp (100%)	accept	acl_outside
77	357	any (100%)	62.59.14.200 (100%)	www (100%)	accept	acl_outside
100	336	172.16.0.25 (100%)	any (100%)	2848 (100%)	accept	acl_inside
89	324	172.16.0.24 (100%)	any (100%)	ftp (100%)	accept	acl_inside
97	254	any (100%)	any (100%)	nntp (100%)	accept	acl_inside
134	150	any (100%)	any (100%)	ssh (100%)	accept	acl_testweb
67	115	69.237.83.3 (100%)	62.59.14.171 (100%)	7777 (100%)	accept	acl_outside
71	115	64.92.205.64/27 (100%)	62.59.14.163 (100%)	smtp (100%)	accept	acl_outside
119	78	any (100%)	any (100%)	7777 (100%)	accept	acl_inside
94	46	any (100%)	any (100%)	telnet (100%)	accept	acl_inside
101	45	any (100%)	any (100%)	7618 (100%)	accept	acl_inside
113	38	any (100%)	any (100%)	5901 (100%)	accept	acl_inside
107	25	any (100%)	any (100%)	h323 (100%)	accept	acl_inside
78	13	any (100%)	62.59.14.200 (100%)	https (100%)	accept	acl_outside

Network Objects Usage

This section shows the aggregate usage of each member for each network group object across all rules that use the object as either Source or Destination based on the access list hit counts. The access list hit counts are available for all rules even if the rules do not have the log option enabled for the rule.

Please note that a CLI script is generated with commands to remove the unused network objects or unused

members of a group object from the firewall. This script can be run on the device using the CLI interface.

Name	Hit Count	Rule(s)	Members/IP Address
db_svcs	8847	84,85	172.16.1.210 (48.9%) 172.16.1.200 (51.1%)

Service Objects Usage

This section shows the aggregate usage of each member for each service group object across all rules that use the object as service based on the access list hit counts. The access list hit counts are available for all rules even if the rules do not have the log option enabled for the rule.

Please note that a CLI script is generated with commands to remove the unused service objects or unused members of an group object from the firewall. This script can be run on the device using the CLI interface.

Name	Hit Count	Type	Rule(s)	Members/Port
web_svcs	18552	group	76,139	www (66.82%) https (33.18%)
inet_svcs	4794	group	141	www (0%) https (0%) smtp (0%) pop3 (0%) domain (100%)
mail_svcs	1723	group	83,140	smtp (43.24%) pop3 (56.76%)

Most Used Rules

This section lists the rules that were found in the access list hit count output, in decreasing order of usage by hit count and percentage hit count. These rules are candidates for being moved toward the beginning of the ruleset to improve performance. Note that moving rules that have order dependencies may cause changes in firewall behavior.

- 64 access-list acl_outside permit tcp any host 62.59.14.171 eq www
Hits=56643 Usage=9.37 %
- 65 access-list acl_outside permit tcp any host 62.59.14.171 eq https
Hits=54267 Usage=8.98 %
- 63 access-list acl_outside permit tcp any host 62.59.14.170 eq www
Hits=48845 Usage=8.08 %
- 59 access-list acl_outside permit tcp any host 62.59.14.161 eq https
Hits=41522 Usage=6.87 %
- 73 access-list acl_outside permit icmp any host 62.59.14.169
Hits=37864 Usage=6.26 %
- 62 access-list acl_outside permit tcp 207.38.18.128 255.255.255.224 host 62.59.14.163 eq smtp
Hits=33468 Usage=5.54 %
- 60 access-list acl_outside permit tcp 216.74.18.32 255.255.255.224 host 62.59.14.163 eq smtp
Hits=25363 Usage=4.2 %
- 58 access-list acl_outside permit tcp any host 62.59.14.161 eq www
Hits=23572 Usage=3.9 %
- 76 access-list acl_outside permit tcp any host 62.59.14.169 object-group web_svcs
Hits=11543 Usage=1.91 %
- 74 access-list acl_outside permit tcp any host 62.59.14.169 eq https
Hits=9736 Usage=1.61 %
- 75 access-list acl_outside permit tcp any host 62.59.14.169 eq 8080
Hits=4423 Usage=0.73 %
- 66 access-list acl_outside permit tcp any host 62.59.14.171 eq ssh

Hits=2253 Usage=0.37 %
61 access-list acl_outside permit tcp host 207.135.79.64 host 62.59.14.169 eq 9595
Hits=1254 Usage=0.21 %
68 access-list acl_outside permit tcp 66.179.26.128 255.255.255.192 host 62.59.14.163 eq smtp
Hits=854 Usage=0.14 %
70 access-list acl_outside permit tcp 216.183.119.96 255.255.255.224 host 62.59.14.163 eq smtp
Hits=698 Usage=0.12 %
69 access-list acl_outside permit tcp 66.179.109.160 255.255.255.224 host 62.59.14.163 eq smtp
Hits=576 Usage=0.1 %
72 access-list acl_outside permit tcp 208.65.144.0 255.255.248.0 host 62.59.14.163 eq smtp
Hits=426 Usage=0.07 %
77 access-list acl_outside permit tcp any host 62.59.14.200 eq www
Hits=357 Usage=0.06 %
67 access-list acl_outside permit tcp host 69.237.83.3 host 62.59.14.171 eq 7777
Hits=115 Usage=0.02 %
71 access-list acl_outside permit tcp 64.92.205.64 255.255.255.224 host 62.59.14.163 eq smtp
Hits=115 Usage=0.02 %
78 access-list acl_outside permit tcp any host 62.59.14.200 eq https
Hits=13 Usage=0.0 %
106 access-list acl_inside permit icmp any any
Hits=26647 Usage=4.41 %
115 access-list acl_inside deny tcp 172.16.0.0 255.255.0.0 any range 1024 65535
Hits=22461 Usage=3.72 %
103 access-list acl_inside permit tcp host 172.16.0.19 any eq smtp
Hits=8857 Usage=1.47 %
108 access-list acl_inside permit udp any any
Hits=8893 Usage=1.47 %
98 access-list acl_inside permit udp host 172.16.0.68 any eq ntp
Hits=7984 Usage=1.32 %
91 access-list acl_inside permit tcp any any eq ftp
Hits=7534 Usage=1.25 %
102 access-list acl_inside permit tcp any any eq 8080
Hits=6846 Usage=1.13 %
87 access-list acl_inside permit tcp any any eq https
Hits=6684 Usage=1.11 %
86 access-list acl_inside permit tcp any any eq www
Hits=3654 Usage=0.6 %
92 access-list acl_inside permit tcp any any eq ssh
Hits=645 Usage=0.11 %
99 access-list acl_inside permit tcp host 172.16.0.25 any eq 2847
Hits=574 Usage=0.09 %
90 access-list acl_inside permit tcp host 172.16.0.24 any eq ssh
Hits=462 Usage=0.08 %
112 access-list acl_inside permit tcp any host 192.168.50.2 eq 5901
Hits=475 Usage=0.08 %
100 access-list acl_inside permit tcp host 172.16.0.25 any eq 2848
Hits=336 Usage=0.06 %
89 access-list acl_inside permit tcp host 172.16.0.24 any eq ftp
Hits=324 Usage=0.05 %
97 access-list acl_inside permit tcp any any eq nntp
Hits=254 Usage=0.04 %
94 access-list acl_inside permit tcp any any eq telnet
Hits=46 Usage=0.01 %
101 access-list acl_inside permit tcp any any eq 7618
Hits=45 Usage=0.01 %
113 access-list acl_inside permit tcp any any eq 5901
Hits=38 Usage=0.01 %
119 access-list acl_inside permit tcp any any eq 7777
Hits=78 Usage=0.01 %
107 access-list acl_inside permit tcp any any eq h323
Hits=25 Usage=0.0 %
82 access-list acl_mail1 permit udp host 192.168.1.2 any eq domain

Hits=55321 Usage=9.15 %
 81 access-list acl_mail1 permit tcp any host 192.168.1.2 eq pop3
Hits=13255 Usage=2.19 %
 84 access-list acl_mail1 permit tcp host 192.168.1.200 object-group db_svcs eq 118
Hits=8847 Usage=1.46 %
 79 access-list acl_mail1 permit tcp any host 192.168.1.4 eq smtp
Hits=7784 Usage=1.29 %
 80 access-list acl_mail1 permit tcp any host 192.168.1.2 eq smtp
Hits=7445 Usage=1.23 %
 137 access-list acl_testweb permit icmp any any
Hits=12674 Usage=2.1 %
 138 access-list acl_testweb permit udp any any eq domain
Hits=8935 Usage=1.48 %
 135 access-list acl_testweb permit tcp any any eq smtp
Hits=5578 Usage=0.92 %
 133 access-list acl_testweb permit tcp any any eq https
Hits=1255 Usage=0.21 %
 132 access-list acl_testweb permit tcp any any eq www
Hits=1212 Usage=0.2 %
 134 access-list acl_testweb permit tcp any any eq ssh
Hits=150 Usage=0.02 %
 142 access-list acl_proxymail permit icmp any any
Hits=11645 Usage=1.93 %
 139 access-list acl_proxymail permit tcp any any object-group web_svcs
Hits=7009 Usage=1.16 %
 141 access-list acl_proxymail permit tcp any any object-group inet_svcs
Hits=4794 Usage=0.79 %
 140 access-list acl_proxymail permit tcp any any object-group mail_svcs
Hits=1723 Usage=0.29 %

Rule Order Dependency

A rule order dependency is a relationship between a pair of rules that affects how the rules can be reordered with respect to one another, without affecting firewall behavior. A rule that is order-dependent on another rule (those rules marked bold below) has overlapping matching ranges with the other rule, and hence cannot be moved above the source of dependency without changing the behavior of the firewall. Similarly a rule that is the source of a dependency cannot be moved below the dependent rule. Thus, a rule order dependency limits rule movement.

Sometimes, two rules that have overlapping matching ranges and the same action, will be marked as order dependent, because one of the two rules may have logging, authentication, nat or other rule options that the other does not have, or is dissimilar. If you ignore such rule options, you may be able to eliminate such order dependencies, thus improving rule reordering. This has to be done by manual inspection.

The next section, that presents a rule reordering based on data in this section, is more conservative in that such rule options are not ignored.

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
83 access-list acl_mail1 deny tcp any host 192.168.1.2 object-group mail_svcs
Order dependent to <80>, <81>
 88 access-list acl_inside permit tcp any any eq 5405
 96 access-list acl_inside permit tcp any any eq 9895
 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
 107 access-list acl_inside permit tcp any any eq h323
 108 access-list acl_inside permit udp any any
 110 access-list acl_inside permit tcp any any eq 5900
 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

```

115  access-list acl_inside deny tcp 172.16.0.0 255.255.0.0 any range 1024 65535
      Order dependent to <88>, <96>, <99>, <100>, <101>, <102>, <107>, <110>, <112>, <113>
116  access-list acl_inside deny udp any any range 135 139
      Order dependent to <108>
119  access-list acl_inside permit tcp any any eq 7777
      Order dependent to <115>

```

Optimized Rule Order

This section suggests a rule ordering for improved firewall performance, based on the rule usage data and rule order dependencies, that does not alter the firewall behavior. The most used rules are moved toward the beginning of the ruleset until they are just below the closest rule that is the source of an order dependency. Use this list to revise your configuration for better performance.

The line numbers shown below refer to the original line numbers in the configuration file.

```

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
63  access-list acl_outside permit tcp any host 62.59.14.170 eq www
59  access-list acl_outside permit tcp any host 62.59.14.161 eq https
73  access-list acl_outside permit icmp any host 62.59.14.169
62  access-list acl_outside permit tcp 207.38.18.128 255.255.255.224 host 62.59.14.163 eq smtp
60  access-list acl_outside permit tcp 216.74.18.32 255.255.255.224 host 62.59.14.163 eq smtp
58  access-list acl_outside permit tcp any host 62.59.14.161 eq www
76  access-list acl_outside permit tcp any host 62.59.14.169 object-group web_svcs
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
66  access-list acl_outside permit tcp any host 62.59.14.171 eq ssh
61  access-list acl_outside permit tcp host 207.135.79.64 host 62.59.14.169 eq 9595
68  access-list acl_outside permit tcp 66.179.26.128 255.255.255.192 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
69  access-list acl_outside permit tcp 66.179.109.160 255.255.255.224 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
77  access-list acl_outside permit tcp any host 62.59.14.200 eq www
67  access-list acl_outside permit tcp host 69.237.83.3 host 62.59.14.171 eq 7777
71  access-list acl_outside permit tcp 64.92.205.64 255.255.255.224 host 62.59.14.163 eq smtp
78  access-list acl_outside permit tcp any host 62.59.14.200 eq https

82  access-list acl_mail1 permit udp host 192.168.1.2 any eq domain
81  access-list acl_mail1 permit tcp any host 192.168.1.2 eq pop3
84  access-list acl_mail1 permit tcp host 192.168.1.200 object-group db_svcs eq 118
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
83  access-list acl_mail1 deny tcp any host 192.168.1.2 object-group mail_svcs
85  access-list acl_mail1 permit udp host 192.168.1.200 object-group db_svcs eq 118

106 access-list acl_inside permit icmp any any
102 access-list acl_inside permit tcp any any eq 8080
99  access-list acl_inside permit tcp host 172.16.0.25 any eq 2847
112 access-list acl_inside permit tcp any host 192.168.50.2 eq 5901
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
113 access-list acl_inside permit tcp any any eq 5901
88  access-list acl_inside permit tcp any any eq 5405
96  access-list acl_inside permit tcp any any eq 9895
107 access-list acl_inside permit tcp any any eq h323
110 access-list acl_inside permit tcp any any eq 5900
115 access-list acl_inside deny tcp 172.16.0.0 255.255.0.0 any range 1024 65535
103 access-list acl_inside permit tcp host 172.16.0.19 any eq smtp
108 access-list acl_inside permit udp any any
98  access-list acl_inside permit udp host 172.16.0.68 any eq ntp

```

```

91 access-list acl_inside permit tcp any any eq ftp
87 access-list acl_inside permit tcp any any eq https
86 access-list acl_inside permit tcp any any eq www
92 access-list acl_inside permit tcp any any eq ssh
90 access-list acl_inside permit tcp host 172.16.0.24 any eq ssh
89 access-list acl_inside permit tcp host 172.16.0.24 any eq ftp
97 access-list acl_inside permit tcp any any eq nntp
94 access-list acl_inside permit tcp any any eq telnet
119 access-list acl_inside permit tcp any any eq 7777
93 access-list acl_inside permit tcp any any eq 81
95 access-list acl_inside permit udp host 172.16.0.68 any eq domain
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
109 access-list acl_inside permit udp host 192.168.5.251 any
111 access-list acl_inside permit udp host 192.168.5.250 any
114 access-list acl_inside permit udp any any eq 5901
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
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

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

137 access-list acl_testweb permit icmp any any
138 access-list acl_testweb permit udp any any eq domain
135 access-list acl_testweb permit tcp any any eq smtp
133 access-list acl_testweb permit tcp any any eq https
132 access-list acl_testweb permit tcp any any eq www
134 access-list acl_testweb permit tcp any any eq ssh
136 access-list acl_testweb permit udp any any eq dnsix

142 access-list acl_proxymail permit icmp any any
139 access-list acl_proxymail permit tcp any any object-group web_svcs
141 access-list acl_proxymail permit tcp any any object-group inet_svcs
140 access-list acl_proxymail permit tcp any any object-group mail_svcs

```

Disabled Rules

This section lists the rules in the configuration that are disabled.

No Rules Found

Time Inactive Rules

This section lists the rules in the configuration that are inactive for some period of time. Rules which are not periodic and which have a time specification older than today are considered as inactive.

No Rules Found

