



Firewall Cleanup and Optimization

Firewall name: FirePac_Example_3
Policy package: RC_Package_Policy

Completed on Fri Apr 16 16:42:23 CDT 2010

This report provides an analysis of the firewall ACL rules based on rule relationships and rule usage obtained from firewall traffic log data. 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.

Log period used for usage analysis is from Thu Oct 08 00:00:01 CDT 2009 till Thu Oct 08 04:00:39 CDT 2009

Configuration Summary

We found a total of 50.86% of rules (59 of 116) that can potentially be removed from the rule base.

Explicit ACL Rules	80
Network Group Objects	8
Network Objects	76
Service Group Objects	56
Service Objects	603

Structural Rule and Object Cleanup

Redundant and Shadowed Rules	15
Unreferenced Network Objects	0
Unreferenced Service Objects	0

Usage-Based Rule and Object Cleanup

Unused Rules	44
Rules without Logging enabled	18
Rule Objects Usage	
Rules with Unused Objects	18
Network Objects Usage	
Unused Network Objects	26
Network Objects with Unused Members	2
Service Objects Usage	
Unused Network Objects	178
Service Objects with Unused Members	3

Rule Optimization

Most Used Rules	72
Rule Order Dependency	26
Optimized Rule Order	

Miscellaneous Rule Attributes

Disabled Rules	8
Time Inactive Rules	0
Rules without comments	10

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](#)

No	Source	Destination	Service	VPN	Action	Track	Comment
*15	Host_Plain_17 2.16.0.24	Any	ftp	Any	accept	None	permit tcp host 172.16.0.24 any eq ftp
	Potentially Redundant to <21>. Review rule options before removal.						
*16	Host_Plain_17 2.16.0.24	Any	ssh	Any	accept	Log	permit tcp host 172.16.0.24 any eq ssh
	Redundant to <23>						
*17	Host_Plain_17 2.16.0.15	Any	ftp	Any	accept	Log	permit tcp host 172.16.0.15 any eq ftp
	Redundant to <21>						
*18	Host_Plain_17 2.16.0.15	Any	ssh	Any	accept	Log	
	Redundant to <23>						
*19	Host_Plain_17 2.16.0.19	Any	ftp	Any	accept	Log	
	Redundant to <21>						
*20	Host_Plain_17 2.16.0.19	Any	ssh	Any	accept	Log	permit tcp host 172.16.0.19 any eq ssh
	Redundant to <23>						
21	Inside_Networ ks	Any	ftp	Any	accept	Log	permit tcp any any eq ftp
23	Inside_Networ ks	Any	ssh	Any	accept	Log	permit tcp any any eq ssh
*26	Host_Plain_17 2.16.0.68	Any	domain-udp	Any	accept	None	
	Redundant to <42>						
*28	Network_172.1 6.0.0_m16	Any	nntp	Any	accept	None	permit tcp 172.16.0.0 255.255.0.0 any eq nntp
	Redundant to <29>						
29	Inside_Networ ks	Any	nntp	Any	accept	None	permit tcp any any eq nntp
*30	Host_Plain_17 2.16.0.68	Any	ntp-udp	Any	accept	None	permit udp host 172.16.0.68 any eq ntp

No	Source	Destination	Service	VPN	Action	Track	Comment
*30							permit udp host 172.16.0.68 any eq ntp
Redundant to <42>							
*37	Host_Plain_19 2.168.5.251	Any	udp_Any	Any	accept	None	permit udp host 192.168.5.251 any
Redundant to <42>							
*38	Host_Plain_19 2.168.5.250	Any	udp_Any	Any	accept	None	permit udp host 192.168.5.250 any
Redundant to <42>							
*40	Inside_Networ ks	Host_Plain_17 2.16.0.4	ntp-udp	Any	accept	None	permit udp any host 172.16.0.4 eq ntp
Redundant to <42>							
42	Inside_Networ ks	Any	udp_Any	Any	accept	None	acl_inside permit udp any any
*44	Inside_Networ ks	Host_Plain_19 2.168.50.2	TCP_Service 5901	Any	accept	Log	permit tcp any host 192.168.50.2 eq 5901
Redundant to <45>							
45	Inside_Networ ks	Any	TCP_Service 5901	Any	accept	Log	permit tcp any any eq 5901
*46	Inside_Networ ks	Any	UDP_Service 5901	Any	accept	Log	permit udp any any eq 5901
Redundant to <37>, <38>, <42>							
78	Range_162.95. 41.18-19	dmz_server	https	Any	accept	Log	permit tcp any host 62.59.14.200 eq https
*79	Host_Ext_mgm t 162.95.41.18	dmz_server	https	Any	drop	Log	permit tcp any host 62.59.14.200 eq https
Shadowed by <78>							

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
No unused network objects found		

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	Match Expression
No unused service objects found			

Unused Rules

This section lists all the rules which have the log option enabled but were not found in any entries in the firewall log. These rules are candidates for removal from the configuration because they may no longer be used. This analysis is only applicable for the period during which the logs were collected, so but were simply not triggered during the logging period. Removing these rules will cause a change in firewall behavior.

Note that there may be some overlap between these rules and those listed in the Redundant and Shadowed Rules section because rules that are made redundant by preceding rules and have the log option enabled will never be present in the firewall log data.

No	Source	Destination	Service	VPN	Action	Track	Comment
16	Host_Plain_17 2.16.0.24	Any	ssh	Any	accept	Log	permit tcp host 172.16.0.24 any eq ssh
17	Host_Plain_17 2.16.0.15	Any	ftp	Any	accept	Log	permit tcp host 172.16.0.15 any eq ftp
18	Host_Plain_17 2.16.0.15	Any	ssh	Any	accept	Log	
19	Host_Plain_17 2.16.0.19	Any	ftp	Any	accept	Log	
20	Host_Plain_17 2.16.0.19	Any	ssh	Any	accept	Log	permit tcp host 172.16.0.19 any eq ssh
22	dmz_testweb_ networks	Any	ssh	Any	accept	Log	permit tcp any any eq ssh
23	Inside_Networ ks	Any	ssh	Any	accept	Log	permit tcp any any eq ssh
27	Inside_Networ ks	Any	TCP_Service 9895	Any	accept	Log	permit tcp any any eq 9895
31	Inside_Networ ks	Any	TCP_Service 7618	Any	accept	Log	
32	Inside_Networ ks	Any	HTTP_and_H TTPS_proxy	Any	accept	Log	tcp any any eq 8080
33	Host_Plain_17 2.16.0.19	Any	smtp	Any	accept	Log	permit tcp host 172.16.0.19 any eq smtp
36	Inside_Networ ks	Any	H323	Any	accept	Log	permit tcp any any eq h323
43	Inside_Networ ks	Any	TCP_Service 5900	Any	accept	Log	permit tcp any any eq 5900
44	Inside_Networ ks	Host_Plain_19 2.168.50.2	TCP_Service 5901	Any	accept	Log	permit tcp any host 192.168.50.2 eq 5901
45	Inside_Networ ks	Any	TCP_Service 5901	Any	accept	Log	permit tcp any any eq 5901
46	Inside_Networ ks	Any	UDP_Service 5901	Any	accept	Log	permit udp any any eq 5901
47	Inside_Networ ks	Any	Napster_direc tory 7777	Any	accept	Log	permit tcp any any eq 7777
50	Host_Plain_19 2.168.1.200	db_svrs	TCP_Service _118	Any	accept	Log	tcp host 192.168.1.200 object-group db_svrs eq 118
51	Host_Plain_19 2.168.1.200	db_svrs	UDP_Service _118	Any	accept	Log	permit udp host 192.168.1.200 object- group db_svrs eq 118
53	dmz_Proxymail networks	Host_Plain_62. 59.14.165	ftp	Any	accept	Log	permit tcp any any object-group mail_svcs
55	dmz_testweb_ networks	Any	UDP_Service 195	Any	accept	Log	
56	dmz_testweb_ networks	Any	Any	Any	drop	Log	
57	Any	Host_Plain_62. 59.14.161	http	Any	accept	Log	permit tcp any host 62.59.14.161 eq www
58	Any	Host_Plain_62. 59.14.161	https	Any	accept	Log	e permit tcp any host 62.59.14.161 eq https
59	Network_216.7 4.18.32_m27	Host_Plain_62. 59.14.163	smtp	Any	accept	Log	permit tcp 216.74.18.32 255.255.255.224 host 62.59.14.163 eq smtp

No	Source	Destination	Service	VPN	Action	Track	Comment
60	Host_Plain_20 7.135.79.64	Host_Plain_62. 59.14.169	TCP_Service _9595	Any	accept	Log	permit tcp host 207.135.79.64 host 62.59.14.169 eq 9595
61	Network_207.3 8.18.128_m27	Host_Plain_62. 59.14.163	smtp	Any	accept	Log	permit tcp 207.38.18.128 255.255.255.224 host 62.59.14.163 eq smtp
62	Any	Host_Plain_62. 59.14.170	http	Any	accept	Log	permit tcp any host 62.59.14.170 eq www
63	Any	Host_Plain_62. 59.14.171	http	Any	accept	Log	permit tcp any host 62.59.14.171 eq www
64	Any	Host_Plain_62. 59.14.171	https	Any	accept	Log	permit tcp any host 62.59.14.171 eq https
65	Any	Host_Plain_62. 59.14.171	ssh	Any	accept	Log	permit tcp any host 62.59.14.171 eq ssh
66	Host_Plain_69. 237.83.3	Host_Plain_62. 59.14.171	Napster_directo ry_7777	Any	accept	Log	permit tcp host 69.237.83.3 host 62.59.14.171 eq 7777
67	Network_66.17 9.26.128_m26	Host_Plain_62. 59.14.163	smtp	Any	accept	Log	permit tcp 66.179.26.128 255.255.255.192 host 62.59.14.163 eq smtp
68	Network_66.17 9.109.160_m2 7	Host_Plain_62. 59.14.163	smtp	Any	accept	Log	permit tcp 66.179.109.160 255.255.255.224 host 62.59.14.163 eq smtp
69	Network_216.1 83.119.96_m2 7	Host_Plain_62. 59.14.163	smtp	Any	accept	Log	permit tcp 216.183.119.96 255.255.255.224 host 62.59.14.163 eq smtp
70	Network_64.92 .205.64_m27	Host_Plain_62. 59.14.163	smtp	Any	accept	Log	permit tcp 64.92.205.64 255.255.255.224 host 62.59.14.163 eq smtp
71	Network_208.6 5.144.0_m21	Host_Plain_62. 59.14.163	smtp	Any	accept	Log	permit tcp 208.65.144.0 255.255.248.0 host 62.59.14.163 eq smtp
74	Any	Host_Plain_62. 59.14.169	HTTP_and_H TTPS_proxy	Any	accept	Log	permit tcp any host 62.59.14.169 eq 8080
75	Any	Host_Plain_62. 59.14.169	web_svcs	Any	accept	Log	permit tcp any host 62.59.14.169 object- group web_svcs
76	Any	Host_Plain_62. 59.14.200	http	Any	accept	Log	permit tcp any host 62.59.14.200 eq www
77	Any	Host_Plain_62. 59.14.200	https	Any	accept	Log	permit tcp any host 62.59.14.200 eq https
78	Range_162.95. 41.18-19	dmz_server	https	Any	accept	Log	permit tcp any host 62.59.14.200 eq https
79	Host_Ext_mgm t_162.95.41.18	dmz_server	https	Any	drop	Log	permit tcp any host 62.59.14.200 eq https
80	Any	Any	Any	Any	drop	Log	

Rules without Logging enabled

This section lists the rules which do not have the log option enabled. These rules are not considered as unused because they will never occur in the firewall log data, even if they are heavily used during the logging period.

No	Source	Destination	Service	VPN	Action	Track	Comment
6	dmz_Proxymail networks	Any	inet_svcs	Any	accept	None	permit tcp any any object-group inet_svcs
8	Inside_Networ ks	Any	http	Any	accept	None	permit tcp any any eq www
15	Host_Plain_17 2.16.0.24	Any	ftp	Any	accept	None	permit tcp host 172.16.0.24 any eq ftp

No	Source	Destination	Service	VPN	Action	Track	Comment
24	Inside_Networks	Any	TCP_Service_81	Any	accept	None	permit tcp any any eq 81
25	Inside_Networks	Any	telnet	Any	accept	None	
26	Host_Plain_172.16.0.68	Any	domain-udp	Any	accept	None	
28	Network_172.16.0.0_m16	Any	nntp	Any	accept	None	permit tcp 172.16.0.0 255.255.0.0 any eq nntp
29	Inside_Networks	Any	nntp	Any	accept	None	permit tcp any any eq nntp
30	Host_Plain_172.16.0.68	Any	ntp-udp	Any	accept	None	permit udp host 172.16.0.68 any eq ntp
34	dmz_testweb_networks	Any	ICMP_Any	Any	accept	None	permit icmp any any
35	Inside_Networks	Any	ICMP_Any	Any	accept	None	permit icmp any any
37	Host_Plain_192.168.5.251	Any	udp_Any	Any	accept	None	permit udp host 192.168.5.251 any
38	Host_Plain_192.168.5.250	Any	udp_Any	Any	accept	None	permit udp host 192.168.5.250 any
40	Inside_Networks	Host_Plain_172.16.0.4	ntp-udp	Any	accept	None	permit udp any host 172.16.0.4 eq ntp
41	dmz_testweb_networks	Any	domain-udp	Any	accept	None	permit udp any any eq domain
42	Inside_Networks	Any	udp_Any	Any	accept	None	acl_inside permit udp any any
49	Host_Plain_192.168.1.2	Any	domain-udp	Any	accept	None	permit udp host 192.168.1.2 any eq domain
72	Any	Host_Plain_62.59.14.169	ICMP_Any	Any	accept	None	permit icmp any host 62.59.14.169

Rule Objects Usage

This section shows the hit counts for each rule along with the percentage usage of each source, destination and service object within the rule based on the log data. The percentage usage shown for an object group includes the rolled up usage for all its members. Objects with zero usage can be removed from the rules. Any rule that has an unused object in Source, Destination and Service, the entire cell is highlighted in Red and the objects with zero usage can be removed from the rule.

Rule No	Hit Count	Source	Destination	Service	Action	Comment
21	4029	Inside_Networks (100%)	Any (100%)	ftp (100%)	accept	permit tcp any any eq ftp
14	1648	Inside_Networks (99.15%)	Any (100%)	TCP_Service_5405 (100%)	accept	permit tcp any any eq 5405
5	1540	dmz_Proxymail_networks (100%)	Any (100%)	ssh (100%)	accept	
13	1200	Network_172.16.0.0_m16 (100%)	Any (100%)	TCP_Service_1024-65535 (100%)	deny	deny tcp 172.16.0.0 255.255.0.0 any range 1024 65535
10	1104	Inside_Networks (100%)	Any (100%)	https (100%)	accept	
12	1100	Host_Plain_172.16.0.25 (100%)	Any (100%)	TCP_Service_2848 (100%)	accept	permit tcp host 172.16.0.25 any eq 2848
4	1034	dmz_mail_networks (100%)	Host_Plain_192.168.1.2 (100%)	mail_svcs (100%)	deny	deny tcp any host 192.168.1.2 object-group mail_svcs
11	1000	Host_Plain_172.16.0.25 (100%)	Any (100%)	TCP_Service_2847 (100%)	accept	permit tcp host 172.16.0.25 any eq 2847

Rule No	Hit Count	Source	Destination	Service	Action	Comment
1	940	dmz_mail_networks (100%)	Host_Plain_192.168.1.4 (100%)	smtp (100%)	accept	permit tcp any host 192.168.1.4 eq smtp
9	842	dmz_testweb_networks (100%)	Any (100%)	https (100%)	accept	permit tcp any any eq https

Network Objects Usage

This section shows the aggregate usage of each network object across all rules that use the object as either Source or Destination based on the log entries. For a network group object, the percentage usage for each immediate member object across all rules that use this member object is shown. The column with "Rule(s) with logging" shows the rules with logging that refer to the object. The column "Rules without logging" refer to the rules without logging that refer to the object. The usage data is available only for those rules with the logging enabled. Hence any objects that are referred in rules without logging cannot be removed even if they have zero usage. These need to be analyzed further by enabling logging and collecting logs and analyzing the usage.

Name	Hit Count	Rule(s) with Logging	Members/IP Address	Rule(s) without Logging
Inside_Networks	6767	10,14,21,23,27,31,32,36,39,43,44,45,46,47,48	Network_192.168.3.0_m24 (6.37%) Network_192.168.4.0_m24 (4.7%) Network_192.168.2.0_m24 (8.08%) Network_10.0.0.0_m8 (12.46%) Network_172.17.0.0_m16 (0%) Network_192.168.5.0_m24 (66.1%) Network_172.16.0.0_m16 (2.29%)	8,24,25,29,35,40,42
Network_192.168.5.0_m24	4473	10,14,21,23,27,31,32,36,39,43,44,45,46,47,48	192.168.5.0/24	8,24,25,29,35,40,42
Host_Plain_172.16.0.25	2100	11,12	172.16.0.25/32	
dmz_mail_networks	1974	1,2,3,4,7,78,79	Network_192.168.1.0_m24 (100%)	
Network_192.168.1.0_m24	1974	1,2,3,4,7,78,79	192.168.1.0/24	
dmz_Proxymail_networks	1540	5,53,54,78,79	Network_192.168.9.0_m24 (100%)	6
Network_192.168.9.0_m24	1540	5,53,54,78,79	192.168.9.0/24	6
Network_172.16.0.0_m16	1355	10,13,14,21,23,27,31,32,36,39,43,44,45,46,47,48	172.16.0.0/16	8,24,25,28,29,35,40,42
Host_Plain_192.168.1.2	1034	2,3,4,78,79	192.168.1.2/32	49
Host_Plain_192.168.1.4	940	1,78,79	192.168.1.4/32	
Network_10.0.0.0_m8	843	10,14,21,23,27,31,32,36,39,43,44,45,46,47,48	10.0.0.0/8	8,24,25,29,35,40,42
dmz_testweb_networks	842	9,22,52,55,56,78,79	Network_192.168.50.0_m24 (100%)	34,41
Network_192.168.50.0_m24	842	9,22,52,55,56,78,79	192.168.50.0/24	34,41
Network_192.168.2.0_m24	547	10,14,21,23,27,31,32,36,39,43,44,45,46,47,48	192.168.2.0/24	8,24,25,29,35,40,42
Network_192.168.3.0_m24	431	10,14,21,23,27,31,32,36,39,43,44,45,46,47,48	192.168.3.0/24	8,24,25,29,35,40,42
Network_192.168.4.0_m24	318	10,14,21,23,27,31,32,36,39,43,44,45,46,47,48	192.168.4.0/24	8,24,25,29,35,40,42

Name	Hit Count	Rule(s) with Logging	Members/IP Address	Rule(s) without Logging
db_svrs	0	50,51	Host_Plain_172.16.1.200 (0%) Host_Plain_172.16.1.210 (0%)	
dmz_server	0	78,79	dmz_testweb_networks (0%) Host_Plain_192.168.1.4 (0%) dmz_Proxymail_networks (0%) Host_Plain_192.168.1.2 (0%) Host_Plain_192.168.1.3 (0%) dmz_mail_networks (0%)	
Host_Ext_mgmt_162.95.41.18	0	79	162.95.41.18/32	
Host_Plain_172.16.0.15	0	17,18	172.16.0.15/32	
Host_Plain_172.16.0.19	0	19,20,33	172.16.0.19/32	
Host_Plain_172.16.0.24	0	16	172.16.0.24/32	15
Host_Plain_172.16.0.4	0		172.16.0.4/32	40
Host_Plain_172.16.0.68	0		172.16.0.68/32	26,30
Host_Plain_172.16.1.200	0	50,51	172.16.1.200/32	
Host_Plain_172.16.1.210	0	50,51	172.16.1.210/32	
Host_Plain_192.168.1.200	0	50,51	192.168.1.200/32	
Host_Plain_192.168.1.3	0	78,79	192.168.1.3/32	
Host_Plain_192.168.5.250	0		192.168.5.250/32	38
Host_Plain_192.168.5.251	0		192.168.5.251/32	37
Host_Plain_192.168.50.2	0	44	192.168.50.2/32	
Host_Plain_207.135.79.64	0	60	207.135.79.64/32	
Host_Plain_62.59.14.161	0	57,58	62.59.14.161/32	
Host_Plain_62.59.14.163	0	59,61,67,68,69,70,71	62.59.14.163/32	
Host_Plain_62.59.14.165	0	53	62.59.14.165/32	
Host_Plain_62.59.14.169	0	60,73,74,75	62.59.14.169/32	72
Host_Plain_62.59.14.170	0	62	62.59.14.170/32	
Host_Plain_62.59.14.171	0	63,64,65,66	62.59.14.171/32	
Host_Plain_62.59.14.200	0	76,77	62.59.14.200/32	
Host_Plain_69.237.8.3.3	0	66	69.237.83.3/32	
Network_172.17.0.0 m16	0	10,14,21,23,27,31,32,36,39,43,44,45,46,47,48	172.17.0.0/16	8,24,25,29,35,40,42
Network_207.38.18.128 m27	0	61	207.38.18.128/27	
Network_208.65.144.0 m21	0	71	208.65.144.0/21	
Network_216.183.119.96 m27	0	69	216.183.119.96/27	
Network_216.74.18.32 m27	0	59	216.74.18.32/27	

Name	Hit Count	Rule(s) with Logging	Members/IP Address	Rule(s) without Logging
Network_64.92.205.64_m27	0	70	64.92.205.64/27	
Network_66.179.109.160_m27	0	68	66.179.109.160/27	
Network_66.179.26.128_m26	0	67	66.179.26.128/26	
Range_162.95.41.18-19	0	78	162.95.41.18-162.95.41.19	

Service Objects Usage

This section shows the aggregate usage of each service object across all rules that use the object as Service based on the log entries. For a service group object, the percentage usage for each member object across all rules that use this member object is shown. The column with "Rule(s) with logging" shows the rules with logging that refer to the object. The column "Rules without logging" refer to the rules without logging that refer to the object. The usage data is available only for those rules with the logging enabled. Hence any objects that are referred in rules without logging cannot be removed even if they have zero usage. These need to be analyzed further by enabling logging and then collecting new logs that indicate how these rules are being used.

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
ftp	4029	tcp	17,19,21,53	21	15
https	1946	tcp	9,10,58,64,73,75,77,78,79	443	6
TCP_Service_5405	1648	tcp	13,14	5405	
ssh	1540	tcp	5,16,18,20,22,23,65	22	
smtp	1530	tcp	1,3,4,33,52,59,61,67,68,69,70,71	25	6
TCP_Service_1024-65535	1200	group	13	pptp-tcp (0%) TCP_Service_4445-4660 (2.5%) TCP_Service_1721-1722 (0%) FW1_netso (2.83%) TCP_Service_5901 (0%) TCP_Service_5900 (0%) TCP_Service_1353-1432 (0%) FW1_ela (0%) Yahoo_Messenger_messages (0%) FW1_ica_services (0%) TCP_Service_5504-5509 (1.25%) TCP_Service_8081-8199 (0%) TCP_Service_1522-1523 (0%) TCP_Service_5101-5189 (0%) Yahoo_Messenger_Webcams (0%) TCP_Service_1112-1211 (0%) TCP_Service_5026-5049 (0%) DameWare (0%) sqlnet1 (0%) TCP_Service_2006-2009 (0%) HTTP and HTTPS proxy	

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
TCP_Service_1024-65535	1200	group	13	(0%) TCP_Service_18233-18261 (0%) FIBMGR (0%) FW1_amon (1%) WinHole (0%) TCP_Service_2627-2648 (0%) Napster_redirector (0%) TCP_Service_7002-7069 (0%) TCP_Service_4667-4999 (0%) DaCryptic (0%) FW1_omi (0%) MySQL (1.75%) Citrix_ICA (0%) CP_reporting (0%) SkyDance-T (0%) TCP_Service_1572-1719 (0%) FW1_ica_push (0%) FW1_CPRID (3.33%) TCP_Service_3307-3388 (0%) TCP_Service_6901-6969 (0%) IPSO_Clustering_Mgmt_Protocol (0.75%) TCP_Service_5051-5099 (0%) Xanadu (0%) GNUtella_TCP (0%) FW1_sds_logon (0%) GNUtella_rtr_TCP (0%) TCP_Service_1082-1096 (1.67%) TCP_Service_1028 (0%) Madster (0%) RealSecure (0%) TCP_Service_8889-9594 (1.5%) TCP_Service_1026 (0%) TCP_Service_65525-65535 (1.33%) TCP_Service_19192-27373 (1.83%) TCP_Service_8201-8874 (2.83%) TCP_Service_1495-1502 (0%) FW1_pslogon_NG (0%) TCP_Service_31786 (0%) TCP_Service_6971-6999 (0%) TCP_Service_18188-18189 (0%) TCP_Service_31793-65523 (0%) GateCrasher (0%) TCP_Service_1864-1999 (0%) TCP_Service_31789 (0%) TCP_Service_27375-31784 (0%) iMesh (0%) TCP_Service_1030 (0%) TCP_Service_5511-5533 (0%)	

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
TCP_Service_1024-65535	1200	group	13	TCP_Service_2011-2048 (0%) TCP_Service_7618 (0%) TCP_Service_4434-4443 (0%) FW1_pslogon (0%) TCP_Service_5632-5899 (0%) InCommand (0%) TCP_Service_31791 (0%) TCP_Service_8876-8887 (0%) TCP_Service_5433-5499 (0%) FW1_cvp (0%) MS-SQL-Monitor (0%) CPML (0%) TCP_Service_1338-1351 (0%) Napster_directory_7777 (0%) OpenWindows (2.08%) TCP_Service_1213 (2.17%) TCP_Service_5191-5404 (0%) CP_rtm (0%) FW1_sam (0%) TCP_Service_3390-3455 (0%) TCP_Service_2650 (0%) Mneah (0%) TCP_Service_5556-5630 (0%) TCP_Service_17301-18180 (0%) Remote_Storm (3.58%) TCP_Service_5902-5999 (0%) AP-Defender (3.42%) TCP_Service_2848 (0%) TCP_Service_2847 (0%) TCP_Service_1036-1073 (0%) ICKiller (0%) TCP_Service_1215-1233 (0%) pcANYWHERE-data (0%) netshow (0%) FW1_ica_pull (0%) TransScout (3.08%) lotus (3.58%) ConnectedOnLine (0%) RainWall_Command (0%) TCP_Service_3003-3305 (1.33%) TCP_Service_2849-2997 (0%) TCP_Service_1099-1110 (0%) Terrortrojan (0%) FW1_uaa (0%) Multidropper (0%) CP_Exnet_PK (0%) TCP_Service_2050-2298 (0%) Orbix-1571 (0%) Orbix-1570 (0%) TCP_Service_1435-1493	

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
TCP_Service_1024-65535	1200	group	13	(0%) TheFlu (0%) TCP_Service_4663-4665 (0%) CPD (0%) Napster_directory_8888_primary (0%) FW1_omi-sic (0%) Remote_Desktop_Protocol (0%) FW1_ica_mgmt_tools (0.92%) OAS-ORB (0%) securidprop (0%) TCP_Service_5535-5554 (0%) TCP_Service_7778-8079 (0%) pcTELECOMMUTE-FileSync (0%) FW1_sds_logon_NG (0%) sqlnet2-1526 (0%) sqlnet2-1525 (0%) H323 (0%) FW1_lea (0%) TCP_Service_9596-9894 (0%) Freak2k (0%) Napster_directory_5555 (2.75%) CP_Exnet_resolve (0%) TCP_Service_9896-16383 (1.83%) TCP_Service_9595 (2.75%) TCP_Service_2652-2846 (0%) TCP_Service_6375-6659 (0%) CPD_amon (0%) Hotline_client (0%) PostgreSQL (1.17%) SubSeven-G (0%) TCP_Service_2999-3000 (2.33%) TCP_Service_6671-6890 (1.83%) TCP_Service_18222-18230 (0%) Kuang2 (0%) nfsd-tcp (0%) TCP_Service_7071-7617 (6.5%) TCP_Service_6348-6373 (7.67%) TCP_Service_3457-3999 (0%) OAS-NameServer (0%) Shadyshell (0%) TCP_Service_1724-1754 (0%) CP_SmartPortal (0%) TCP_Service_5405 (0%) TCP_Service_18206 (2.25%) TCP_Service_1756-1862 (0%) StoneBeat-Daemon (0%) TCP_Service_18209 (0%)	

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
TCP_Service_1024-65535	1200	group	13	Real-Audio (3%) TCP_Service_1504-1520 (0%) UltorsTrojan (0%) RAT (2.92%) TCP_Service_18203-18204 (0%) CP_redundant (0%) GoToMyPC (4.67%) TCP_Service_1235-1242 (0%) MSN_Messenger_File_Transfer (0%) TCP_Service_6130-6345 (1.5%) TCP_Service_5001-5024 (0%) TCP_Service_4001-4432 (0%) TCP_Service_2300-2625 (0%) TCP_Service_18212-18220 (0%) TCP_Service_2001-2003 (0%) X11 (0%) TCP_Service_18267-19189 (2.08%) T.120 (2.92%) Napster_directory_4444 (2.75%) Trinoo (2.58%) HackaTack_31790 (0%) HackaTack_31792 (0%) MSNMS (0%) TCP_Service_1527-1569 (0%) MS-SQL-Server (0%) irc1 (0%) eDonkey_4661 (0%) eDonkey_4662 (0%) TCP_Service_1244-1336 (0%) StoneBeat-Control (0%) irc2 (3.17%) CP_seam (0%) TCP_Service_6064-6128 (0%) TCP_Service_1075-1080 (0%) TCP_Service_18194-18201 (0%) TCP_Service_1032-1034 (0%) TCP_Service_16385-17299 (0%) SubSeven (0%) Jade (0%) AOL (2.58%) Kaos (0%) FW1_ufp (0%) HackaTack_31788 (0%) KaZaA (0%) HackaTack_31787 (0%) TCP_Service_7619-7776 (0%) TCP_Service_9895 (0%) HackaTack_31785 (0%) TCP_Service_5406-5431	

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
TCP_Service_1024-65535	1200	group	13	(0%)	
TCP_Service_2848	1100	tcp	12,13	2848	
mail_svcs	1034	group	4	smtp (57.06%) pop-3 (42.94%)	
TCP_Service_2847	1000	tcp	11,13	2847	
pop-3	444	tcp	2,4	110	6
TCP_Service_6348-6373	92	tcp	13	6348-6373	
TCP_Service_7071-7617	78	tcp	13	7071-7617	
GoToMyPC	56	tcp	13	8200	
lotus	43	tcp	13	1352	
Remote_Storm	43	tcp	13	1025	
AP-Defender	41	tcp	13	2626	
FW1_CPRID	40	tcp	13	18208	
irc2	38	tcp	13	7000	
TransScout	37	tcp	13	2004-2005	
Real-Audio	36	tcp	13	7070	
RAT	35	tcp	13	1097-1098	
T.120	35	tcp	13	1503	
FW1_netso	34	tcp	13	19190	
TCP_Service_8201-8874	34	tcp	13	8201-8874	
Napster_directory_4444	33	tcp	13	4444	
Napster_directory_5555	33	tcp	13	5555	
TCP_Service_9595	33	tcp	13,60	9595	
AOL	31	tcp	13	5190	
Trinoo	31	tcp	13	1524	
TCP_Service_4445-4660	30	tcp	13	4445-4660	
TCP_Service_2999-3000	28	tcp	13	2999-3000	
TCP_Service_18206	27	tcp	13	18206	
TCP_Service_1213	26	tcp	13	1213	
OpenWindows	25	tcp	13	2000	
TCP_Service_18267-19189	25	tcp	13	18267-19189	
TCP_Service_19192-27373	22	tcp	13	19192-27373	
TCP_Service_6671-6890	22	tcp	13	6671-6890	
TCP_Service_9896-16383	22	tcp	13	9896-16383	
MySQL	21	tcp	13	3306	
TCP_Service_1082-1096	20	tcp	13	1082-1096	
TCP_Service_6130-6345	18	tcp	13	6130-6345	
TCP_Service_8889-9594	18	tcp	13	8889-9594	
TCP_Service_3003-3305	16	tcp	13	3003-3305	
TCP_Service_65525	16	tcp	13	65525-65535	

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
-65535	16	tcp	13	65525-65535	
TCP_Service_5504-5509	15	tcp	13	5504-5509	
PostgreSQL	14	tcp	13	5432	
FW1_amon	12	tcp	13	18193	
FW1_ica_mgmt_tools	11	tcp	13	18265	
IPSO_Clustering_Mgmt_Protocol	9	tcp	13	1111	
archie	0	udp		1525	37,38,42
biff	0	udp		512	37,38,42
Blubster	0	udp		41170	37,38,42
bootp	0	udp		67	37,38,42
Citrix_ICA	0	tcp	13	1494	
ConnectedOnLine	0	tcp	13	16384	
CP_Exnet_PK	0	tcp	13	18262	
CP_Exnet_resolve	0	tcp	13	18263	
CP_redundant	0	tcp	13	18221	
CP_reporting	0	tcp	13	18205	
CP_rtm	0	tcp	13	18202	
CP_seam	0	tcp	13	18266	
CP_SmartPortal	0	tcp	13	4433	
CPD	0	tcp	13	18191	
CPD_amon	0	tcp	13	18192	
CPMI	0	tcp	13	18190	
CU-SeeMe	0	udp		7648-7652	37,38,42
DaCryptic	0	tcp	13	1074	
DameWare	0	tcp	13	6129	
daytime-udp	0	udp		13	37,38,42
dest-unreach	0	icmp		3/Destination Unreachable	34,35,72
Direct_Connect_UDP	0	udp		411-412	37,38,42
discard-udp	0	udp		9	37,38,42
domain-tcp	0	tcp		53	6
domain-udp	0	udp		53	26,37,38,41,42,49
E2ECP	0	udp		18241	37,38,42
echo-reply	0	icmp		0/Echo Reply	34,35,72
echo-request	0	icmp		8/Echo	34,35,72
echo-udp	0	udp		7	37,38,42
eDonkey_4661	0	tcp	13	4661	
eDonkey_4662	0	tcp	13	4662	
eDonkey_4665	0	udp		4665	37,38,42
FIBMGR	0	tcp	13	2010	
Freak2k	0	tcp	13	7001	
FW1_cvp	0	tcp	13	18181	

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
FW1_ela	0	tcp	13	18187	
FW1_ica_pull	0	tcp	13	18210	
FW1_ica_push	0	tcp	13	18211	
FW1_ica_services	0	tcp	13	18264	
FW1_lea	0	tcp	13	18184	
FW1_load_agent	0	udp		18212	37,38,42
FW1_omi	0	tcp	13	18185	
FW1_omi-sic	0	tcp	13	18186	
FW1_pslogon	0	tcp	13	18207	
FW1_pslogon_NG	0	tcp	13	18231	
FW1_sam	0	tcp	13	18183	
FW1_scv_keep_alive	0	udp		18233	37,38,42
FW1_sds_logon	0	tcp	13	18232	
FW1_sds_logon_NG	0	tcp	13	65524	
FW1_snmp	0	udp		260	37,38,42
FW1_uaa	0	tcp	13	19191	
FW1_ufp	0	tcp	13	18182	
GateCrasher	0	tcp	13	6970	
GNUtella_rtr_TCP	0	tcp	13	6347	
GNUtella_rtr_UDP	0	udp		6347	37,38,42
GNUtella_TCP	0	tcp	13	6346	
GNUtella_UDP	0	udp		6346	37,38,42
H323	0	tcp	13,36	1720	
H323_ras_only	0	udp		1719	37,38,42
HackaTack_31785	0	tcp	13	31785	
HackaTack_31787	0	tcp	13	31787	
HackaTack_31788	0	tcp	13	31788	
HackaTack_31789	0	udp		31789	37,38,42
HackaTack_31790	0	tcp	13	31790	
HackaTack_31791	0	udp		31791	37,38,42
HackaTack_31792	0	tcp	13	31792	
Hotline_client	0	tcp	13	5500-5503	
Hotline_tracker	0	udp		5499	37,38,42
http	0	tcp	57,62,63,75,76	80	6,8
HTTP_and_HTTPS_proxy	0	tcp	13,32,74	8080	
ICKiller	0	tcp	13	1027	
ICMP_Any	0	group		source-quench (0%) timestamp-reply (0%) info-req (0%) echo-reply (0%) time-exceeded (0%) mask-reply (0%) echo-request (0%) param-prblm (0%) timestamp (0%)	34,35,72

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
ICMP_Any	0	group		mask-request (0%) info-reply (0%) dest-unreach (0%) redirect (0%)	34,35,72
ICQ_locator	0	udp		4000	37,38,42
IKE	0	udp		500	37,38,42
IKE_NAT_TRAVER SAL	0	udp		4500	37,38,42
iMesh	0	tcp	13	5000	
InCommand	0	tcp	13	1029	
inet_svcs	0	group		https (0%) smtp (0%) pop-3 (0%) http (0%) domain-tcp (0%)	6
info-reply	0	icmp		16/Information Reply	34,35,72
info-req	0	icmp		15/Information Request	34,35,72
interphone	0	udp		22555	37,38,42
irc1	0	tcp	13	6660-6670	
Jade	0	tcp	13	1024	
Kaos	0	tcp	13	1212	
KaZaA	0	tcp	13	1214	
Kerberos_v5_UDP	0	udp		88	37,38,42
kerberos-udp	0	udp		750	37,38,42
Kuang2	0	tcp	13	17300	
L2TP	0	udp		1701	37,38,42
Madster	0	tcp	13	5025	
mask-reply	0	icmp		18/Address Mask Reply	34,35,72
mask-request	0	icmp		17/Address Mask Request	34,35,72
microsoft-ds-udp	0	udp		445	37,38,42
Mneah	0	tcp	13	4666	
MSN_Messenger_1 863_UDP	0	udp		1863	37,38,42
MSN_Messenger_5 190	0	udp		5190	37,38,42
MSN_Messenger_Fil e Transfer	0	tcp	13	6891-6900	
MSN_Messenger_V oice	0	udp		6901	37,38,42
MSNMS	0	tcp	13	1863	
MS-SQL-Monitor	0	tcp	13	1434	
MS-SQL- Monitor_UDP	0	udp		1434	37,38,42
MS-SQL-Server	0	tcp	13	1433	
MS-SQL- Server_UDP	0	udp		1433	37,38,42
Multidropper	0	tcp	13	1035	
name	0	udp		42	37,38,42
Napster_directory_7 777	0	tcp	13,47,66	7777	
Napster_directory_8 888_primary	0	tcp	13	8888	
Napster_redirector	0	tcp	13	8875	

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
nbdatagram	0	udp	39	138	37,38,42
nbname	0	udp	39	137	37,38,42
netshow	0	tcp	13	1755	
NEW-RADIUS	0	udp		1812	37,38,42
NEW-RADIUS-ACCOUNTING	0	udp		1813	37,38,42
nfsd	0	udp		2049	37,38,42
nfsd-tcp	0	tcp	13	2049	
nntp	0	tcp		119	28,29
NoBackO	0	udp		1201	37,38,42
ntp-udp	0	udp		123	30,37,38,40,42
OAS-NameServer	0	tcp	13	2649	
OAS-ORB	0	tcp	13	2651	
Orbix-1570	0	tcp	13	1570	
Orbix-1571	0	tcp	13	1571	
param-prblm	0	icmp		12/Parameter Problem	34,35,72
pcANYWHERE-data	0	tcp	13	5631	
pcANYWHERE-stat	0	udp		5632	37,38,42
pcTELECOMMUTE-FileSync	0	tcp	13	2299	
pptp-tcp	0	tcp	13	1723	
RADIUS	0	udp		1645	37,38,42
RADIUS-ACCOUNTING	0	udp		1646	37,38,42
RainWall_Command	0	tcp	13	6374	
RainWall_Daemon	0	udp		6372	37,38,42
RainWall_Status	0	udp		6374	37,38,42
RainWall_Stop	0	udp		6373	37,38,42
RDP	0	udp		259	37,38,42
RealSecure	0	tcp	13	2998	
redirect	0	icmp		5/Redirect	34,35,72
Remote_Desktop_Protocol	0	tcp	13	3389	
RexxRave	0	udp		1104	37,38,42
rip	0	udp		520	37,38,42
RIPng	0	udp		521	37,38,42
securidprop	0	tcp	13	5510	
securid-udp	0	udp		5500	37,38,42
Shadyshell	0	tcp	13	1337	
SkyDance-T	0	tcp	13	4000	
snmp	0	udp		161	37,38,42
snmp-trap	0	udp		162	37,38,42
source-quench	0	icmp		4/Source Quench	34,35,72
sqlnet1	0	tcp	13	1521	
sqlnet2-1525	0	tcp	13	1525	

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
sqlnet2-1526	0	tcp	13	1526	
StoneBeat-Control	0	tcp	13	3002	
StoneBeat-Daemon	0	tcp	13	3001	
SubSeven	0	tcp	13	27374	
SubSeven-G	0	tcp	13	1243	
SWTP_Gateway	0	udp		9281	37,38,42
SWTP_SMS	0	udp		9282	37,38,42
syslog	0	udp		514	37,38,42
TACACS	0	udp		49	37,38,42
TCP_Service_1026	0	tcp	13	1026	
TCP_Service_1028	0	tcp	13	1028	
TCP_Service_1030	0	tcp	13	1030	
TCP_Service_1032-1034	0	tcp	13	1032-1034	
TCP_Service_1036-1073	0	tcp	13	1036-1073	
TCP_Service_1075-1080	0	tcp	13	1075-1080	
TCP_Service_1099-1110	0	tcp	13	1099-1110	
TCP_Service_1112-1211	0	tcp	13	1112-1211	
TCP_Service_118	0	tcp	50	118	
TCP_Service_1215-1233	0	tcp	13	1215-1233	
TCP_Service_1235-1242	0	tcp	13	1235-1242	
TCP_Service_1244-1336	0	tcp	13	1244-1336	
TCP_Service_1338-1351	0	tcp	13	1338-1351	
TCP_Service_1353-1432	0	tcp	13	1353-1432	
TCP_Service_1435-1493	0	tcp	13	1435-1493	
TCP_Service_1495-1502	0	tcp	13	1495-1502	
TCP_Service_1504-1520	0	tcp	13	1504-1520	
TCP_Service_1522-1523	0	tcp	13	1522-1523	
TCP_Service_1527-1569	0	tcp	13	1527-1569	
TCP_Service_1572-1719	0	tcp	13	1572-1719	
TCP_Service_16385-17299	0	tcp	13	16385-17299	
TCP_Service_1721-1722	0	tcp	13	1721-1722	
TCP_Service_1724-1754	0	tcp	13	1724-1754	
TCP_Service_17301-18180	0	tcp	13	17301-18180	
TCP_Service_1756-1862	0	tcp	13	1756-1862	
TCP_Service_18188-18189	0	tcp	13	18188-18189	
TCP_Service_18194-18201	0	tcp	13	18194-18201	
TCP_Service_18203-18204	0	tcp	13	18203-18204	

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
TCP_Service_18209	0	tcp	13	18209	
TCP_Service_18212-18220	0	tcp	13	18212-18220	
TCP_Service_18222-18230	0	tcp	13	18222-18230	
TCP_Service_18233-18261	0	tcp	13	18233-18261	
TCP_Service_1864-1999	0	tcp	13	1864-1999	
TCP_Service_2001-2003	0	tcp	13	2001-2003	
TCP_Service_2006-2009	0	tcp	13	2006-2009	
TCP_Service_2011-2048	0	tcp	13	2011-2048	
TCP_Service_2050-2298	0	tcp	13	2050-2298	
TCP_Service_2300-2625	0	tcp	13	2300-2625	
TCP_Service_2627-2648	0	tcp	13	2627-2648	
TCP_Service_2650	0	tcp	13	2650	
TCP_Service_2652-2846	0	tcp	13	2652-2846	
TCP_Service_27375-31784	0	tcp	13	27375-31784	
TCP_Service_2849-2997	0	tcp	13	2849-2997	
TCP_Service_31786	0	tcp	13	31786	
TCP_Service_31789	0	tcp	13	31789	
TCP_Service_31791	0	tcp	13	31791	
TCP_Service_31793-65523	0	tcp	13	31793-65523	
TCP_Service_3307-3388	0	tcp	13	3307-3388	
TCP_Service_3390-3455	0	tcp	13	3390-3455	
TCP_Service_3457-3999	0	tcp	13	3457-3999	
TCP_Service_4001-4432	0	tcp	13	4001-4432	
TCP_Service_4434-4443	0	tcp	13	4434-4443	
TCP_Service_4663-4665	0	tcp	13	4663-4665	
TCP_Service_4667-4999	0	tcp	13	4667-4999	
TCP_Service_5001-5024	0	tcp	13	5001-5024	
TCP_Service_5026-5049	0	tcp	13	5026-5049	
TCP_Service_5051-5099	0	tcp	13	5051-5099	
TCP_Service_5101-5189	0	tcp	13	5101-5189	
TCP_Service_5191-5404	0	tcp	13	5191-5404	
TCP_Service_5406-5431	0	tcp	13	5406-5431	
TCP_Service_5433-5499	0	tcp	13	5433-5499	
TCP_Service_5511-5533	0	tcp	13	5511-5533	
TCP_Service_5535-5554	0	tcp	13	5535-5554	
TCP_Service_5556-5630	0	tcp	13	5556-5630	

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
TCP_Service_5632-5899	0	tcp	13	5632-5899	
TCP_Service_5900	0	tcp	13,43	5900	
TCP_Service_5901	0	tcp	13,44,45	5901	
TCP_Service_5902-5999	0	tcp	13	5902-5999	
TCP_Service_6064-6128	0	tcp	13	6064-6128	
TCP_Service_6375-6659	0	tcp	13	6375-6659	
TCP_Service_6901-6969	0	tcp	13	6901-6969	
TCP_Service_6971-6999	0	tcp	13	6971-6999	
TCP_Service_7002-7069	0	tcp	13	7002-7069	
TCP_Service_7618	0	tcp	13,31	7618	
TCP_Service_7619-7776	0	tcp	13	7619-7776	
TCP_Service_7778-8079	0	tcp	13	7778-8079	
TCP_Service_8081-8199	0	tcp	13	8081-8199	
TCP_Service_81	0	tcp		81	24
TCP_Service_8876-8887	0	tcp	13	8876-8887	
TCP_Service_9596-9894	0	tcp	13	9596-9894	
TCP_Service_9895	0	tcp	13,27	9895	
telnet	0	tcp		23	25
Terrortrojan	0	tcp	13	3456	
tftp	0	udp		69	37,38,42
TheFlu	0	tcp	13	5534	
time-exceeded	0	icmp		11/Time Exceeded	34,35,72
timestamp	0	icmp		13/Timestamp	34,35,72
timestamp-reply	0	icmp		14/Timestamp Reply	34,35,72
time-udp	0	udp		37	37,38,42
tunnel_test	0	udp		18234	37,38,42
udp_Any	0	group		UDP_Service_1105-1200 (0%) UDP_Service_1814-1862 (0%) archie (0%) MSN_Messenger_1863_UDP (0%) MS-SQL-Server_UDP (0%) echo-udp (0%) MSN_Messenger_Voice (0%) daytime-udp (0%) UDP_Service_4666-4999 (0%) UDP_Service_446-499 (0%) UDP_Service_1-6 (0%) UDP_Service_4501-4664 (0%) RainWall_Status (0%) bootp (0%)	37,38,42

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
udp_Any	0	group		UDP_Service_8 (0%) discard-udp (0%) ntp-udp (0%) Kerberos_v5_UDP (0%) tftp (0%) tunnel_test (0%) UDP_Service_5633-6256 (0%) VPN1_IPSEC_encapsulation (0%) UDP_Service_5501-5631 (0%) MSN_Messenger_5190 (0%) time-udp (0%) UDP_Service_6348-6371 (0%) FW1_scv_keep_alive (0%) UDP_Service_14-36 (0%) RainWall_Daemon (0%) nbdatagram (0%) UDP_Service_119-122 (0%) MS-SQL-Monitor_UDP (0%) UDP_Service_1864-2048 (0%) UDP_Service_1647-1700 (0%) UDP_Service_1720-1811 (0%) UDP_Service_68 (0%) UDP_Service_6375-6900 (0%) UDP_Service_18242-22554 (0%) UDP_Service_6902-7647 (0%) FW1_snmp (0%) UDP_Service_89-117 (0%) UDP_Service_7653-9280 (0%) UDP_Service_31790 (0%) TACACS (0%) syslog (0%) UDP_Service_501-511 (0%) H323_ras_only (0%) SWTP_SMS (0%) UDP_Service_124-136 (0%) kerberos-udp (0%) RADIUS (0%) interphone (0%) SWTP_Gateway (0%) UDP_Service_261-410 (0%) UDP_Service_2747-3999 (0%) UDP_Service_2050-2745 (0%) UDP_Service_41171-65535 (0%) who (0%) NEW-RADIUS (0%) UDP_Service_18235-18240 (0%)	37,38,42

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
udp_Any	0	group		UDP_Service_1202-1432 (0%) UDP_Service_118 (0%) FW1_load_agent (0%) UDP_Service_70-87 (0%) NEW-RADIUS-ACCOUNTING (0%) UDP_Service_5191-5498 (0%) UDP_Service_751-1103 (0%) UDP_Service_31792-41169 (0%) UDP_Service_38-41 (0%) snmp (0%) GNUtella_UDP (0%) WinMX (0%) E2ECP (0%) CU-SeeMe (0%) nbname (0%) domain-udp (0%) UDP_Service_522-749 (0%) RIPng (0%) UDP_Service_18213-18232 (0%) RexxRave (0%) UDP_Service_1526-1644 (0%) UDP_Service_413-444 (0%) Blubster (0%) microsoft-ds-udp (0%) Direct_Connect_UDP (0%) UDP_Service_6258-6345 (0%) UDP_Service_54-66 (0%) pcANYWHERE-stat (0%) securid-udp (0%) UDP_Service_50-52 (0%) RADIUS-ACCOUNTING (0%) IKE_NAT_TRAVERSAL (0%) UDP_Service_4001-4499 (0%) HackaTack_31791 (0%) name (0%) UDP_Service_9283-18211 (0%) UDP_Service_5011-5189 (0%) UDP_Service_43-48 (0%) UDP_Service_1702-1718 (0%) rip (0%) UDP_Service_22556-31788 (0%) HackaTack_31789 (0%) Yahoo_Messenger_Voice_Chat_UDP (0%) eDonkey_4665 (0%) snmp-trap (0%) UDP_Service_163-258 (0%) UDP_Service_10-12 (0%) RainWall_Stop (0%) L2TP (0%)	37,38,42

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
udp_Any	0	group		RDP (0%) NoBackO (0%) IKE (0%) UDP_Service_1435-1524 (0%) Hotline_tracker (0%) GNUtella_rtr_UDP (0%) ICQ_locator (0%) nfsd (0%) UDP_Service_515-519 (0%) UDP_Service_139-160 (0%) biff (0%)	37,38,42
UDP_Service_10-12	0	udp		10-12	37,38,42
UDP_Service_1105-1200	0	udp		1105-1200	37,38,42
UDP_Service_118	0	udp	51	118	37,38,42
UDP_Service_119-122	0	udp		119-122	37,38,42
UDP_Service_1202-1432	0	udp		1202-1432	37,38,42
UDP_Service_124-136	0	udp		124-136	37,38,42
UDP_Service_135-136	0	udp	39	135-136	
UDP_Service_135-139	0	group	39	UDP_Service_139 (0%) nbname (0%) UDP_Service_135-136 (0%) nbdatagram (0%)	
UDP_Service_139	0	udp	39	139	
UDP_Service_139-160	0	udp		139-160	37,38,42
UDP_Service_1435-1524	0	udp		1435-1524	37,38,42
UDP_Service_14-36	0	udp		14-36	37,38,42
UDP_Service_1526-1644	0	udp		1526-1644	37,38,42
UDP_Service_1-6	0	udp		1-6	37,38,42
UDP_Service_163-258	0	udp		163-258	37,38,42
UDP_Service_1647-1700	0	udp		1647-1700	37,38,42
UDP_Service_1702-1718	0	udp		1702-1718	37,38,42
UDP_Service_1720-1811	0	udp		1720-1811	37,38,42
UDP_Service_1814-1862	0	udp		1814-1862	37,38,42
UDP_Service_18213-18232	0	udp		18213-18232	37,38,42
UDP_Service_18235-18240	0	udp		18235-18240	37,38,42
UDP_Service_18242-22554	0	udp		18242-22554	37,38,42
UDP_Service_1864-2048	0	udp		1864-2048	37,38,42
UDP_Service_195	0	udp	55	195	
UDP_Service_2050-2745	0	udp		2050-2745	37,38,42
UDP_Service_22556-31788	0	udp		22556-31788	37,38,42
UDP_Service_261-410	0	udp		261-410	37,38,42

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
UDP_Service_2747-3999	0	udp		2747-3999	37,38,42
UDP_Service_31790	0	udp		31790	37,38,42
UDP_Service_31792-41169	0	udp		31792-41169	37,38,42
UDP_Service_38-41	0	udp		38-41	37,38,42
UDP_Service_4001-4499	0	udp		4001-4499	37,38,42
UDP_Service_41171-65535	0	udp		41171-65535	37,38,42
UDP_Service_413-444	0	udp		413-444	37,38,42
UDP_Service_43-48	0	udp		43-48	37,38,42
UDP_Service_446-499	0	udp		446-499	37,38,42
UDP_Service_4501-4664	0	udp		4501-4664	37,38,42
UDP_Service_4666-4999	0	udp		4666-4999	37,38,42
UDP_Service_5011-5189	0	udp		5011-5189	37,38,42
UDP_Service_501-511	0	udp		501-511	37,38,42
UDP_Service_50-52	0	udp		50-52	37,38,42
UDP_Service_515-519	0	udp		515-519	37,38,42
UDP_Service_5191-5498	0	udp		5191-5498	37,38,42
UDP_Service_522-749	0	udp		522-749	37,38,42
UDP_Service_54-66	0	udp		54-66	37,38,42
UDP_Service_5501-5631	0	udp		5501-5631	37,38,42
UDP_Service_5633-6256	0	udp		5633-6256	37,38,42
UDP_Service_5901	0	udp	46	5901	
UDP_Service_6258-6345	0	udp		6258-6345	37,38,42
UDP_Service_6348-6371	0	udp		6348-6371	37,38,42
UDP_Service_6375-6900	0	udp		6375-6900	37,38,42
UDP_Service_68	0	udp		68	37,38,42
UDP_Service_6902-7647	0	udp		6902-7647	37,38,42
UDP_Service_70-87	0	udp		70-87	37,38,42
UDP_Service_751-1103	0	udp		751-1103	37,38,42
UDP_Service_7653-9280	0	udp		7653-9280	37,38,42
UDP_Service_8	0	udp		8	37,38,42
UDP_Service_89-117	0	udp		89-117	37,38,42
UDP_Service_9283-18211	0	udp		9283-18211	37,38,42
UltorsTrojan	0	tcp	13	1234	
VPN1_IPSEC_encapsulation	0	udp		2746	37,38,42
web_svcs	0	group	75	https (0%) http (0%)	
who	0	udp		513	37,38,42
WinHole	0	tcp	13	1081	

Name	Hit Count	Type	Rule(s) with Logging	Members/Port	Rule(s) without Logging
WinMX	0	udp		6257	37,38,42
X11	0	tcp	13	6000-6063	
Xanadu	0	tcp	13	1031	
Yahoo_Messenger_messages	0	tcp	13	5050	
Yahoo_Messenger_Voice_Chat_UDP	0	udp		5000-5010	37,38,42
Yahoo_Messenger_Webcams	0	tcp	13	5100	

Most Used Rules

This section lists the rules that were found in the firewall log data for the logging data, 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.

No	Source	Destination	Service	VPN	Action	Track	Hits (%)
21	Inside_Networks	Any	ftp	Any	accept	Log	4029 (27.91)
14	Inside_Networks	Any	TCP_Service_5405	Any	accept	Log	1648 (11.42)
5	dmz_Proxymail_networks	Any	ssh	Any	accept	Log	1540 (10.67)
13	Network_172.16.0.0_m16	Any	TCP_Service_1024-65535	Any	drop	Log	1200 (8.31)
10	Inside_Networks	Any	https	Any	accept	Log	1104 (7.65)
12	Host_Plain_172.16.0.25	Any	TCP_Service_2848	Any	accept	Log	1100 (7.62)
4	dmz_mail_networks	Host_Plain_192.168.1.2	mail_svcs	Any	drop	Log	1034 (7.16)
11	Host_Plain_172.16.0.25	Any	TCP_Service_2847	Any	accept	Log	1000 (6.93)
1	dmz_mail_networks	Host_Plain_192.168.1.4	smtp	Any	accept	Log	940 (6.51)
9	dmz_testweb_networks	Any	https	Any	accept	Log	842 (5.83)
15	Host_Plain_172.16.0.24	Any	ftp	Any	accept	None	0 (0.0)
16	Host_Plain_172.16.0.24	Any	ssh	Any	accept	Log	0 (0.0)
17	Host_Plain_172.16.0.15	Any	ftp	Any	accept	Log	0 (0.0)
18	Host_Plain_172.16.0.15	Any	ssh	Any	accept	Log	0 (0.0)
19	Host_Plain_172.16.0.19	Any	ftp	Any	accept	Log	0 (0.0)
20	Host_Plain_172.16.0.19	Any	ssh	Any	accept	Log	0 (0.0)
22	dmz_testweb_networks	Any	ssh	Any	accept	Log	0 (0.0)
23	Inside_Networks	Any	ssh	Any	accept	Log	0 (0.0)
24	Inside_Networks	Any	TCP_Service_81	Any	accept	None	0 (0.0)
25	Inside_Networks	Any	telnet	Any	accept	None	0 (0.0)
26	Host_Plain_172.16.0.68	Any	domain-udp	Any	accept	None	0 (0.0)

No	Source	Destination	Service	VPN	Action	Track	Hits (%)
27	Inside_Networks	Any	TCP_Service_9895	Any	accept	Log	0 (0.0)
28	Network_172.16.0.0_m16	Any	nntp	Any	accept	None	0 (0.0)
29	Inside_Networks	Any	nntp	Any	accept	None	0 (0.0)
30	Host_Plain_172.16.0.68	Any	ntp-udp	Any	accept	None	0 (0.0)
31	Inside_Networks	Any	TCP_Service_7618	Any	accept	Log	0 (0.0)
32	Inside_Networks	Any	HTTP_and_HTTPS_proxy	Any	accept	Log	0 (0.0)
33	Host_Plain_172.16.0.19	Any	smtp	Any	accept	Log	0 (0.0)
34	dmz_testweb_networks	Any	ICMP_Any	Any	accept	None	0 (0.0)
35	Inside_Networks	Any	ICMP_Any	Any	accept	None	0 (0.0)
36	Inside_Networks	Any	H323	Any	accept	Log	0 (0.0)
37	Host_Plain_192.168.5.251	Any	udp_Any	Any	accept	None	0 (0.0)
38	Host_Plain_192.168.5.250	Any	udp_Any	Any	accept	None	0 (0.0)
40	Inside_Networks	Host_Plain_172.16.0.4	ntp-udp	Any	accept	None	0 (0.0)
41	dmz_testweb_networks	Any	domain-udp	Any	accept	None	0 (0.0)
42	Inside_Networks	Any	udp_Any	Any	accept	None	0 (0.0)
43	Inside_Networks	Any	TCP_Service_5900	Any	accept	Log	0 (0.0)
44	Inside_Networks	Host_Plain_192.168.50.2	TCP_Service_5901	Any	accept	Log	0 (0.0)
45	Inside_Networks	Any	TCP_Service_5901	Any	accept	Log	0 (0.0)
46	Inside_Networks	Any	UDP_Service_5901	Any	accept	Log	0 (0.0)
47	Inside_Networks	Any	Napster_directory_7777	Any	accept	Log	0 (0.0)
49	Host_Plain_192.168.1.2	Any	domain-udp	Any	accept	None	0 (0.0)
50	Host_Plain_192.168.1.200	db_svrs	TCP_Service_118	Any	accept	Log	0 (0.0)
51	Host_Plain_192.168.1.200	db_svrs	UDP_Service_118	Any	accept	Log	0 (0.0)
53	dmz_Proxymail_networks	Host_Plain_62.59.14.165	ftp	Any	accept	Log	0 (0.0)
55	dmz_testweb_networks	Any	UDP_Service_195	Any	accept	Log	0 (0.0)
56	dmz_testweb_networks	Any	Any	Any	drop	Log	0 (0.0)
57	Any	Host_Plain_62.59.14.161	http	Any	accept	Log	0 (0.0)
58	Any	Host_Plain_62.59.14.161	https	Any	accept	Log	0 (0.0)
59	Network_216.74.18.32_m27	Host_Plain_62.59.14.163	smtp	Any	accept	Log	0 (0.0)
6	dmz_Proxymail_networks	Any	inet_svcs	Any	accept	None	0 (0.0)
60	Host_Plain_207.135.79.64	Host_Plain_62.59.14.169	TCP_Service_9595	Any	accept	Log	0 (0.0)
61	Network_207.38.18.128_m27	Host_Plain_62.59.14.163	smtp	Any	accept	Log	0 (0.0)
62	Any	Host_Plain_62.59.14.170	http	Any	accept	Log	0 (0.0)
63	Any	Host_Plain_62.59.14.171	http	Any	accept	Log	0 (0.0)

No	Source	Destination	Service	VPN	Action	Track	Hits (%)
64	Any	Host_Plain_62.59.14.171	https	Any	accept	Log	0 (0.0)
65	Any	Host_Plain_62.59.14.171	ssh	Any	accept	Log	0 (0.0)
66	Host_Plain_69.237.83.3	Host_Plain_62.59.14.171	Napster_directory_7777	Any	accept	Log	0 (0.0)
67	Network_66.17.9.26.128_m26	Host_Plain_62.59.14.163	smtp	Any	accept	Log	0 (0.0)
68	Network_66.17.9.109.160_m27	Host_Plain_62.59.14.163	smtp	Any	accept	Log	0 (0.0)
69	Network_216.183.119.96_m27	Host_Plain_62.59.14.163	smtp	Any	accept	Log	0 (0.0)
70	Network_64.92.205.64_m27	Host_Plain_62.59.14.163	smtp	Any	accept	Log	0 (0.0)
71	Network_208.65.144.0_m21	Host_Plain_62.59.14.163	smtp	Any	accept	Log	0 (0.0)
72	Any	Host_Plain_62.59.14.169	ICMP_Any	Any	accept	None	0 (0.0)
74	Any	Host_Plain_62.59.14.169	HTTP_and_HTTPS_proxy	Any	accept	Log	0 (0.0)
75	Any	Host_Plain_62.59.14.169	web_svcs	Any	accept	Log	0 (0.0)
76	Any	Host_Plain_62.59.14.200	http	Any	accept	Log	0 (0.0)
77	Any	Host_Plain_62.59.14.200	https	Any	accept	Log	0 (0.0)
78	Range_162.95.41.18-19	dmz_server	https	Any	accept	Log	0 (0.0)
79	Host_Ext_mgmt_162.95.41.18	dmz_server	https	Any	drop	Log	0 (0.0)
8	Inside_Networks	Any	http	Any	accept	None	0 (0.0)
80	Any	Any	Any	Any	drop	Log	0 (0.0)

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.

No	Source	Destination	Service	VPN	Action	Track	Comment
1	dmz_mail_networks	Host_Plain_192.168.1.4	smtp	Any	accept	Log	permit tcp any host 192.168.1.4 eq smtp
5	dmz_Proxymail_networks	Any	ssh	Any	accept	Log	

No	Source	Destination	Service	VPN	Action	Track	Comment
5							
6	dmz_Proxymail_networks	Any	inet_svcs	Any	accept	None	permit tcp any any object-group inet_svcs
8	Inside_Networks	Any	http	Any	accept	None	permit tcp any any eq www
9	dmz_testweb_networks	Any	https	Any	accept	Log	permit tcp any any eq https
10	Inside_Networks	Any	https	Any	accept	Log	
11	Host_Plain_17_2.16.0.25	Any	TCP_Service_2847	Any	accept	Log	permit tcp host 172.16.0.25 any eq 2847
12	Host_Plain_17_2.16.0.25	Any	TCP_Service_2848	Any	accept	Log	permit tcp host 172.16.0.25 any eq 2848
*13	Network_172.16.0.0_m16	Any	TCP_Service_1024-65535	Any	drop	Log	deny tcp 172.16.0.0 255.255.0.0 any range 1024 65535
Order dependent to <11>, <12>							
*14	Inside_Networks	Any	TCP_Service_5405	Any	accept	Log	permit tcp any any eq 5405
Order dependent to <13>							
15	Host_Plain_17_2.16.0.24	Any	ftp	Any	accept	None	permit tcp host 172.16.0.24 any eq ftp
16	Host_Plain_17_2.16.0.24	Any	ssh	Any	accept	Log	permit tcp host 172.16.0.24 any eq ssh
17	Host_Plain_17_2.16.0.15	Any	ftp	Any	accept	Log	permit tcp host 172.16.0.15 any eq ftp
18	Host_Plain_17_2.16.0.15	Any	ssh	Any	accept	Log	
19	Host_Plain_17_2.16.0.19	Any	ftp	Any	accept	Log	
20	Host_Plain_17_2.16.0.19	Any	ssh	Any	accept	Log	permit tcp host 172.16.0.19 any eq ssh
*21	Inside_Networks	Any	ftp	Any	accept	Log	permit tcp any any eq ftp
Order dependent to <15>							
22	dmz_testweb_networks	Any	ssh	Any	accept	Log	permit tcp any any eq ssh
23	Inside_Networks	Any	ssh	Any	accept	Log	permit tcp any any eq ssh
24	Inside_Networks	Any	TCP_Service_81	Any	accept	None	permit tcp any any eq 81
25	Inside_Networks	Any	telnet	Any	accept	None	
26	Host_Plain_17_2.16.0.68	Any	domain-udp	Any	accept	None	
*27	Inside_Networks	Any	TCP_Service_9895	Any	accept	Log	permit tcp any any eq 9895
Order dependent to <13>							
28	Network_172.16.0.0_m16	Any	nntp	Any	accept	None	permit tcp 172.16.0.0 255.255.0.0 any eq nntp
29	Inside_Networks	Any	nntp	Any	accept	None	permit tcp any any eq nntp
30	Host_Plain_17_2.16.0.68	Any	ntp-udp	Any	accept	None	permit udp host 172.16.0.68 any eq ntp
*31	Inside_Networks	Any	TCP_Service_7618	Any	accept	Log	
Order dependent to <13>							
*32	Inside_Networks	Any	HTTP_and_HTTPS_proxy	Any	accept	Log	tcp any any eq 8080
Order dependent to <13>							
33	Host_Plain_17_2.16.0.19	Any	smtp	Any	accept	Log	permit tcp host 172.16.0.19 any eq smtp
34	dmz_testweb_networks	Any	ICMP_Any	Any	accept	None	permit icmp any any

No	Source	Destination	Service	VPN	Action	Track	Comment
35	Inside_Networks	Any	ICMP_Any	Any	accept	None	permit icmp any any
*36	Inside_Networks	Any	H323	Any	accept	Log	permit tcp any any eq h323
Order dependent to <13>							
37	Host_Plain_19 2.168.5.251	Any	udp_Any	Any	accept	None	permit udp host 192.168.5.251 any
38	Host_Plain_19 2.168.5.250	Any	udp_Any	Any	accept	None	permit udp host 192.168.5.250 any
40	Inside_Networks	Host_Plain_17 2.16.0.4	ntp-udp	Any	accept	None	permit udp any host 172.16.0.4 eq ntp
41	dmz_testweb_networks	Any	domain-udp	Any	accept	None	permit udp any any eq domain
42	Inside_Networks	Any	udp_Any	Any	accept	None	acl_inside permit udp any any
*43	Inside_Networks	Any	TCP_Service 5900	Any	accept	Log	permit tcp any any eq 5900
Order dependent to <13>							
*44	Inside_Networks	Host_Plain_19 2.168.50.2	TCP_Service 5901	Any	accept	Log	permit tcp any host 192.168.50.2 eq 5901
Order dependent to <13>							
*45	Inside_Networks	Any	TCP_Service 5901	Any	accept	Log	permit tcp any any eq 5901
Order dependent to <13>							
*46	Inside_Networks	Any	UDP_Service 5901	Any	accept	Log	permit udp any any eq 5901
Order dependent to <37>, <38>, <42>							
*47	Inside_Networks	Any	Napster_directory 7777	Any	accept	Log	permit tcp any any eq 7777
Order dependent to <13>							
49	Host_Plain_19 2.168.1.2	Any	domain-udp	Any	accept	None	permit udp host 192.168.1.2 any eq domain
50	Host_Plain_19 2.168.1.200	db_svrs	TCP_Service _118	Any	accept	Log	tcp host 192.168.1.200 object-group db_svrs eq 118
51	Host_Plain_19 2.168.1.200	db_svrs	UDP_Service _118	Any	accept	Log	permit udp host 192.168.1.200 object-group db_svrs eq 118
53	dmz_Proxymail_networks	Host_Plain_62. 59.14.165	ftp	Any	accept	Log	permit tcp any any object-group mail_svcs
55	dmz_testweb_networks	Any	UDP_Service 195	Any	accept	Log	
*56	dmz_testweb_networks	Any	Any	Any	drop	Log	
Order dependent to <9>, <22>, <34>, <41>, <55>							
*57	Any	Host_Plain_62. 59.14.161	http	Any	accept	Log	permit tcp any host 62.59.14.161 eq www
Order dependent to <6>, <8>, <56>							
*58	Any	Host_Plain_62. 59.14.161	https	Any	accept	Log	e permit tcp any host 62.59.14.161 eq https
Order dependent to <6>, <56>							
59	Network_216.7 4.18.32_m27	Host_Plain_62. 59.14.163	smtp	Any	accept	Log	permit tcp 216.74.18.32 255.255.255.224 host 62.59.14.163 eq smtp
60	Host_Plain_20 7.135.79.64	Host_Plain_62. 59.14.169	TCP_Service _9595	Any	accept	Log	permit tcp host 207.135.79.64 host 62.59.14.169 eq 9595
61	Network_207.3 8.18.128_m27	Host_Plain_62. 59.14.163	smtp	Any	accept	Log	permit tcp 207.38.18.128 255.255.255.224 host 62.59.14.163 eq smtp
*62	Any	Host_Plain_62. 59.14.170	http	Any	accept	Log	permit tcp any host 62.59.14.170 eq www
Order dependent to <6>, <8>, <56>							

No	Source	Destination	Service	VPN	Action	Track	Comment
*63	Any	Host_Plain_62.59.14.171	http	Any	accept	Log	permit tcp any host 62.59.14.171 eq www
Order dependent to <6>, <8>, <56>							
*64	Any	Host_Plain_62.59.14.171	https	Any	accept	Log	permit tcp any host 62.59.14.171 eq https
Order dependent to <6>, <56>							
*65	Any	Host_Plain_62.59.14.171	ssh	Any	accept	Log	permit tcp any host 62.59.14.171 eq ssh
Order dependent to <56>							
66	Host_Plain_69.237.83.3	Host_Plain_62.59.14.171	Napster_directory_7777	Any	accept	Log	permit tcp host 69.237.83.3 host 62.59.14.171 eq 7777
67	Network_66.179.26.128	Host_Plain_62.59.14.163	smtp	Any	accept	Log	permit tcp 66.179.26.128 host 62.59.14.163 eq smtp
68	Network_66.179.109.160	Host_Plain_62.59.14.163	smtp	Any	accept	Log	permit tcp 66.179.109.160 host 62.59.14.163 eq smtp
69	Network_216.183.119.96	Host_Plain_62.59.14.163	smtp	Any	accept	Log	permit tcp 216.183.119.96 host 62.59.14.163 eq smtp
70	Network_64.92.205.64	Host_Plain_62.59.14.163	smtp	Any	accept	Log	permit tcp 64.92.205.64 host 62.59.14.163 eq smtp
71	Network_208.65.144.0	Host_Plain_62.59.14.163	smtp	Any	accept	Log	permit tcp 208.65.144.0 host 62.59.14.163 eq smtp
*72	Any	Host_Plain_62.59.14.169	ICMP_Any	Any	accept	None	permit icmp any host 62.59.14.169
Order dependent to <56>							
*74	Any	Host_Plain_62.59.14.169	HTTP_and_HTTPS_proxy	Any	accept	Log	permit tcp any host 62.59.14.169 eq 8080
Order dependent to <13>, <56>							
*75	Any	Host_Plain_62.59.14.169	web_svcs	Any	accept	Log	permit tcp any host 62.59.14.169 object-group web_svcs
Order dependent to <6>, <8>, <56>							
*76	Any	Host_Plain_62.59.14.200	http	Any	accept	Log	permit tcp any host 62.59.14.200 eq www
Order dependent to <6>, <8>, <56>							
*77	Any	Host_Plain_62.59.14.200	https	Any	accept	Log	permit tcp any host 62.59.14.200 eq https
Order dependent to <6>, <56>							
78	Range_162.95.41.18-19	dmz_server	https	Any	accept	Log	permit tcp any host 62.59.14.200 eq https
*79	Host_Ext_mgmt_162.95.41.18	dmz_server	https	Any	drop	Log	permit tcp any host 62.59.14.200 eq https
Order dependent to <78>							
*80	Any	Any	Any	Any	drop	Log	
Order dependent to <1>, <5>, <6>, <8>, <9>, <10>, <11>, <12>, <14>, <15>, <16>, <17>, <18>, <19>, <20>, <21>, <22>, <23>, <24>, <25>, <26>, <27>, <28>, <29>, <30>, <31>, <32>, <33>, <34>, <35>, <36>, <37>, <38>, <40>, <41>, <42>, <43>, <44>, <45>, <46>, <47>, <49>, <50>, <51>, <53>, <55>, <57>, <58>, <59>, <60>, <61>, <62>, <63>, <64>, <65>, <66>, <67>, <68>, <69>, <70>, <71>, <72>, <74>, <75>, <76>, <77>, <78>							

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.

No	Orig No	Source	Destination	Service	VPN	Action	Track	Comment
1	15	Host_Plain_17 2.16.0.24	Any	ftp	Any	accept	None	permit tcp host 172.16.0.24 any eq ftp
2	21	Inside_Networ ks	Any	ftp	Any	accept	Log	permit tcp any any eq ftp
3	12	Host_Plain_17 2.16.0.25	Any	TCP_Service_ 2848	Any	accept	Log	permit tcp host 172.16.0.25 any eq 2848
4	11	Host_Plain_17 2.16.0.25	Any	TCP_Service_ 2847	Any	accept	Log	permit tcp host 172.16.0.25 any eq 2847
5	13	Network_172.1 6.0.0_m16	Any	TCP_Service_ 1024-65535	Any	drop	Log	deny tcp 172.16.0.0 255.255.0.0 any range 1024 65535
6	14	Inside_Networ ks	Any	TCP_Service_ 5405	Any	accept	Log	permit tcp any any eq 5405
7	5	dmz_Proxymail networks	Any	ssh	Any	accept	Log	
8	10	Inside_Networ ks	Any	https	Any	accept	Log	
9	4	dmz_mail_net works	Host_Plain_1 92.168.1.2	mail_svcs	Any	drop	Log	deny tcp any host 192.168.1.2 object-group mail_svcs
10	1	dmz_mail_net works	Host_Plain_1 92.168.1.4	smtp	Any	accept	Log	permit tcp any host 192.168.1.4 eq smtp
11	9	dmz_testweb_ networks	Any	https	Any	accept	Log	permit tcp any any eq https
12	6	dmz_Proxymail networks	Any	inet_svcs	Any	accept	None	permit tcp any any object- group inet_svcs
13	8	Inside_Networ ks	Any	http	Any	accept	None	permit tcp any any eq www
14	16	Host_Plain_17 2.16.0.24	Any	ssh	Any	accept	Log	permit tcp host 172.16.0.24 any eq ssh
15	17	Host_Plain_17 2.16.0.15	Any	ftp	Any	accept	Log	permit tcp host 172.16.0.15 any eq ftp
16	18	Host_Plain_17 2.16.0.15	Any	ssh	Any	accept	Log	
17	19	Host_Plain_17 2.16.0.19	Any	ftp	Any	accept	Log	
18	20	Host_Plain_17 2.16.0.19	Any	ssh	Any	accept	Log	permit tcp host 172.16.0.19 any eq ssh
19	22	dmz_testweb_ networks	Any	ssh	Any	accept	Log	permit tcp any any eq ssh
20	23	Inside_Networ ks	Any	ssh	Any	accept	Log	permit tcp any any eq ssh
21	24	Inside_Networ ks	Any	TCP_Service_ 81	Any	accept	None	permit tcp any any eq 81
22	25	Inside_Networ ks	Any	telnet	Any	accept	None	
23	26	Host_Plain_17 2.16.0.68	Any	domain-udp	Any	accept	None	
24	27	Inside_Networ ks	Any	TCP_Service_ 9895	Any	accept	Log	permit tcp any any eq 9895
25	28	Network_172.1 6.0.0_m16	Any	nntp	Any	accept	None	permit tcp 172.16.0.0 255.255.0.0 any eq nntp
26	29	Inside_Networ ks	Any	nntp	Any	accept	None	permit tcp any any eq nntp
27	30	Host_Plain_17 2.16.0.68	Any	ntp-udp	Any	accept	None	permit udp host 172.16.0.68 any eq ntp
28	31	Inside_Networ ks	Any	TCP_Service_ 7618	Any	accept	Log	
29	32	Inside_Networ ks	Any	HTTP_and_HT TPS_proxy	Any	accept	Log	tcp any any eq 8080
30	33	Host_Plain_17 2.16.0.19	Any	smtp	Any	accept	Log	permit tcp host 172.16.0.19 any eq smtp

No	Orig No	Source	Destination	Service	VPN	Action	Track	Comment
30								permit tcp host 172.16.0.19 any eq smtp
31	34	dmz_testweb_networks	Any	ICMP_Any	Any	accept	None	permit icmp any any
32	35	Inside_Networks	Any	ICMP_Any	Any	accept	None	permit icmp any any
33	36	Inside_Networks	Any	H323	Any	accept	Log	permit tcp any any eq h323
34	37	Host_Plain_192.168.5.251	Any	udp_Any	Any	accept	None	permit udp host 192.168.5.251 any
35	38	Host_Plain_192.168.5.250	Any	udp_Any	Any	accept	None	permit udp host 192.168.5.250 any
36	40	Inside_Networks	Host_Plain_172.16.0.4	ntp-udp	Any	accept	None	permit udp any host 172.16.0.4 eq ntp
37	41	dmz_testweb_networks	Any	domain-udp	Any	accept	None	permit udp any any eq domain
38	42	Inside_Networks	Any	udp_Any	Any	accept	None	acl_inside permit udp any any
39	43	Inside_Networks	Any	TCP_Service_5900	Any	accept	Log	permit tcp any any eq 5900
40	44	Inside_Networks	Host_Plain_192.168.50.2	TCP_Service_5901	Any	accept	Log	permit tcp any host 192.168.50.2 eq 5901
41	45	Inside_Networks	Any	TCP_Service_5901	Any	accept	Log	permit tcp any any eq 5901
42	46	Inside_Networks	Any	UDP_Service_5901	Any	accept	Log	permit udp any any eq 5901
43	47	Inside_Networks	Any	Napster_directory_7777	Any	accept	Log	permit tcp any any eq 7777
44	49	Host_Plain_192.168.1.2	Any	domain-udp	Any	accept	None	permit udp host 192.168.1.2 any eq domain
45	50	Host_Plain_192.168.1.200	db_svrs	TCP_Service_118	Any	accept	Log	tcp host 192.168.1.200 object-group db_svrs eq 118
46	51	Host_Plain_192.168.1.200	db_svrs	UDP_Service_118	Any	accept	Log	permit udp host 192.168.1.200 object-group db_svrs eq 118
47	53	dmz_Proxymail_networks	Host_Plain_62.59.14.165	ftp	Any	accept	Log	permit tcp any any object-group mail_svcs
48	55	dmz_testweb_networks	Any	UDP_Service_195	Any	accept	Log	
49	56	dmz_testweb_networks	Any	Any	Any	drop	Log	
50	57	Any	Host_Plain_62.59.14.161	http	Any	accept	Log	permit tcp any host 62.59.14.161 eq www
51	58	Any	Host_Plain_62.59.14.161	https	Any	accept	Log	e permit tcp any host 62.59.14.161 eq https
52	59	Network_216.74.18.32_m27	Host_Plain_62.59.14.163	smtp	Any	accept	Log	permit tcp 216.74.18.32 255.255.255.224 host 62.59.14.163 eq smtp
53	60	Host_Plain_207.135.79.64	Host_Plain_62.59.14.169	TCP_Service_9595	Any	accept	Log	permit tcp host 207.135.79.64 host 62.59.14.169 eq 9595
54	61	Network_207.38.18.128_m27	Host_Plain_62.59.14.163	smtp	Any	accept	Log	permit tcp 207.38.18.128 255.255.255.224 host 62.59.14.163 eq smtp
55	62	Any	Host_Plain_62.59.14.170	http	Any	accept	Log	permit tcp any host 62.59.14.170 eq www
56	63	Any	Host_Plain_62.59.14.171	http	Any	accept	Log	permit tcp any host 62.59.14.171 eq www
57	64	Any	Host_Plain_62.59.14.171	https	Any	accept	Log	permit tcp any host 62.59.14.171 eq https
58	65	Any	Host_Plain_62.59.14.171	ssh	Any	accept	Log	permit tcp any host 62.59.14.171 eq ssh
59	66	Host_Plain_69.237.83.3	Host_Plain_62.59.14.171	Napster_directory_7777	Any	accept	Log	permit tcp host 69.237.83.3 host 62.59.14.171 eq 7777
60	67	Network_66.179.26.128_m26	Host_Plain_62.59.14.163	smtp	Any	accept	Log	permit tcp 66.179.26.128 255.255.255.192 host 62.59.14.163 eq smtp

No	Orig No	Source	Destination	Service	VPN	Action	Track	Comment
61	68	Network_66.179.109.160_m27	Host_Plain_62.59.14.163	smtp	Any	accept	Log	permit tcp 66.179.109.160 255.255.255.224 host 62.59.14.163 eq smtp
62	69	Network_216.183.119.96_m27	Host_Plain_62.59.14.163	smtp	Any	accept	Log	permit tcp 216.183.119.96 255.255.255.224 host 62.59.14.163 eq smtp
63	70	Network_64.92.205.64_m27	Host_Plain_62.59.14.163	smtp	Any	accept	Log	permit tcp 64.92.205.64 255.255.255.224 host 62.59.14.163 eq smtp
64	71	Network_208.65.144.0_m21	Host_Plain_62.59.14.163	smtp	Any	accept	Log	permit tcp 208.65.144.0 255.255.248.0 host 62.59.14.163 eq smtp
65	72	Any	Host_Plain_62.59.14.169	ICMP_Any	Any	accept	None	permit icmp any host 62.59.14.169
66	74	Any	Host_Plain_62.59.14.169	HTTP_and_HTTPS_proxy	Any	accept	Log	permit tcp any host 62.59.14.169 eq 8080
67	75	Any	Host_Plain_62.59.14.169	web_svcs	Any	accept	Log	permit tcp any host 62.59.14.169 object-group web_svcs
68	76	Any	Host_Plain_62.59.14.200	http	Any	accept	Log	permit tcp any host 62.59.14.200 eq www
69	77	Any	Host_Plain_62.59.14.200	https	Any	accept	Log	permit tcp any host 62.59.14.200 eq https
70	78	Range_162.95.41.18-19	dmz_server	https	Any	accept	Log	permit tcp any host 62.59.14.200 eq https
71	79	Host_Ext_mgmt_162.95.41.18	dmz_server	https	Any	drop	Log	permit tcp any host 62.59.14.200 eq https
72	80	Any	Any	Any	Any	drop	Log	

Disabled Rules

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

No	Source	Destination	Service	VPN	Action	Track	Comment
2	dmz_mail_networks	Host_Plain_192.168.1.2	pop-3	Any	accept	Log	DISABLED
3	dmz_mail_networks	Host_Plain_192.168.1.2	smtp	Any	accept	Log	permit tcp any host 192.168.1.2 eq smtp DISABLED
7	dmz_mail_networks	Any	Any	Any	drop	Log	DISABLED
39	Inside_Networks	Any	UDP_Service_135-139	Any	drop	Log	deny udp any any range 135 139 DISABLED
48	Inside_Networks	Any	Any	Any	drop	Log	DISABLED
52	dmz_testweb_networks	Any	smtp	Any	accept	Log	tcp any any eq smtp DISABLED
54	dmz_Proxymail_networks	Any	Any	Any	drop	Log	Auto-generated implied any any drop rule at end of ACL DISABLED
73	Any	Host_Plain_62.59.14.169	https	Any	accept	Log	permit tcp any host 62.59.14.169 eq https DISABLED

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	Source	Destination	Service	VPN	Action	Time	Comment
No Data							

Rules without comments

This section lists the rules in the configuration that do not have comments.

No	Source	Destination	Service	VPN	Action	Track	Comment
5	dmz_Proxymail_networks	Any	ssh	Any	accept	Log	
10	Inside_Networks	Any	https	Any	accept	Log	
18	Host_Plain_17_2.16.0.15	Any	ssh	Any	accept	Log	
19	Host_Plain_17_2.16.0.19	Any	ftp	Any	accept	Log	
25	Inside_Networks	Any	telnet	Any	accept	None	
26	Host_Plain_17_2.16.0.68	Any	domain-udp	Any	accept	None	
31	Inside_Networks	Any	TCP_Service_7618	Any	accept	Log	
55	dmz_testweb_networks	Any	UDP_Service_195	Any	accept	Log	
56	dmz_testweb_networks	Any	Any	Any	drop	Log	
80	Any	Any	Any	Any	drop	Log	