Firewall Risk Analysis Report - FireFind

File Analyzed: CLIENT1 Firewall Rules - Anonymised - Firewall Policy-INSIDE-FW01 - WITH RISK FEEDE

Total Rules Analyzed: 60

Total Risks Found: 76

Info Risks: 19

High Risks: 36

Medium Risks: 23

Critical Risks: 17

Rule ID	Issue	Field	Value	Severity
1	No issues found	-	-	INFO
2	No issues found	-	-	INFO
3	No issues found	-	-	INFO
4	Weak protocol	service	http	HIGH
5	No issues found	-	-	INFO
6	suspicious_service	service	ldap	HIGH
6	suspicious_service	service	ldap	HIGH
7	suspicious_service	service	smtp	HIGH
7	No logging error	log	no log	MEDIUM
8	allow all service	service	all	HIGH
8	allow all service	action	accept	HIGH
9	allow all service	service	all	HIGH
9	allow all service	action	accept	HIGH
9	No logging error	log	no log	MEDIUM
10	No logging error	log	no log	MEDIUM
11	allow all service	service	all	HIGH
11	allow all service	action	accept	HIGH
12	suspicious_service	service	smtp	HIGH
12	No logging error	log	no log	MEDIUM
13	No logging error	log	no log	MEDIUM

14	LPD Port Exposure	service	lpdw0rm	HIGH
14	No logging error	log	no log	MEDIUM
15	No issues found	-	-	INFO
16	No issues found	-	-	INFO
17	allow all service	service	all	HIGH
17	allow all service	action	accept	HIGH
17	No logging error	log	no log	MEDIUM
18	No issues found	-	-	INFO
19	No issues found	-	-	INFO
20	No logging error	log	no log	MEDIUM
21	No logging error	log	no log	MEDIUM
22	No issues found	-	-	INFO
23	allow all service	service	all	HIGH
23	allow all service	action	accept	HIGH
24	LPD Port Exposure	service	lpdw0rm	HIGH
24	No logging error	log	no log	MEDIUM
25	No logging error	log	no log	MEDIUM
26	No issues found	-	-	INFO
27	Weak protocol	service	ftp	HIGH
28	No issues found	-	-	INFO
29	No issues found	-	-	INFO
30	smb Netbios Exposed	service	135	CRITICAL
30	smb Netbios Exposed	service	445	CRITICAL
31	smb Netbios Exposed	service	135	CRITICAL
31	smb Netbios Exposed	service	445	CRITICAL
32	smb Netbios Exposed	service	135	CRITICAL
32	smb Netbios Exposed	service	445	CRITICAL
33	allow all service	service	all	HIGH
33	allow all service	action	accept	HIGH
34	Admin Port Exposed	service	22	CRITICAL
34	Admin Port Exposed	service	23	CRITICAL

34	Weak protocol	service	telnet	HIGH
35	Admin Port Exposed	service	22	CRITICAL
35	No logging error	log	no log	MEDIUM
36	Admin Port Exposed	service	22	CRITICAL
36	Admin Port Exposed	service	23	CRITICAL
36	No logging error	log	no log	MEDIUM
36	Weak protocol	service	telnet	HIGH
37	Weak protocol	service	http	HIGH
38	No issues found	-	-	INFO
39	Admin Port Exposed	service	23	CRITICAL
39	No logging error	log	no log	MEDIUM
39	Weak protocol	service	telnet	HIGH
40	No issues found	-	-	INFO
41	allow all service	service	all	HIGH
41	allow all service	action	accept	HIGH
41	No logging error	log	no log	MEDIUM
42	No issues found	-	-	INFO
43	No logging error	log	no log	MEDIUM
44	No issues found	-	-	INFO
45	No logging error	log	no log	MEDIUM
45	Weak protocol	service	http	HIGH
46	No logging error	log	no log	MEDIUM
46	Weak protocol	service	ftp	HIGH
47	No logging error	log	no log	MEDIUM
48	Weak protocol	service	http	HIGH
49	No logging error	log	no log	MEDIUM
50	Admin Port Exposed	service	3389	CRITICAL
50	No logging error	log	no log	MEDIUM
50	Weak protocol	service	http	HIGH
51	Weak protocol	service	http	HIGH
52	Weak protocol	service	http	HIGH

53	Admin Port Exposed	service	22	CRITICAL
53	Admin Port Exposed	service	23	CRITICAL
53	Admin Port Exposed	service	3389	CRITICAL
53	No logging error	log	no log	MEDIUM
53	Weak protocol	service	telnet	HIGH
54	No logging error	log	no log	MEDIUM
54	Weak protocol	service	http	HIGH
55	No issues found	-	-	INFO
56	No issues found	-	-	INFO
57	No issues found	-	-	INFO
58	Weak protocol	service	http	HIGH
59	Weak protocol	service	http	HIGH
60	Admin Port Exposed	service	22	CRITICAL