Firewall Risk Analysis Report - FireFind

FIREFIND RISK DETECTOR
TRISKELE LABS

Triskele Labs

Summary of the Risk Analysis

Metric	Value
File Analyzed	CLIENT1 Firewall Rules - Anonymised - Firewall Policy-INSIDE-FW01 - WITH RISK
File Belongs to	Client 1 Or 3 Xlsx
Total Rules Analyzed	60
Total Risks Found	76
No Risks	19
High Risks	22
Medium Risks	37
Critical Risks	17
Analyzed Date and Time	2025-10-03 15:03:59

Rules by Severity

- CRITICAL 17.9%
- No Risks 20.0%
- MEDIUM 38.9%
- HIGH 23.2%
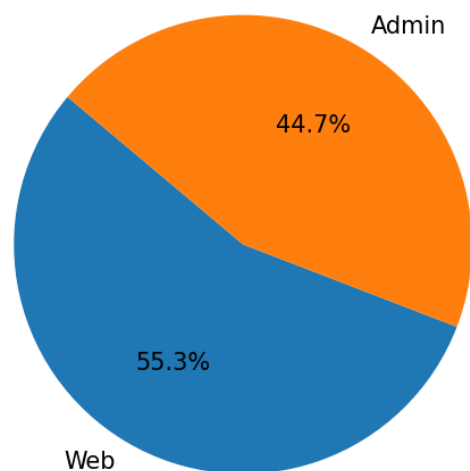
Rules by Category

- Admin 44.7%
- Web 55.3%
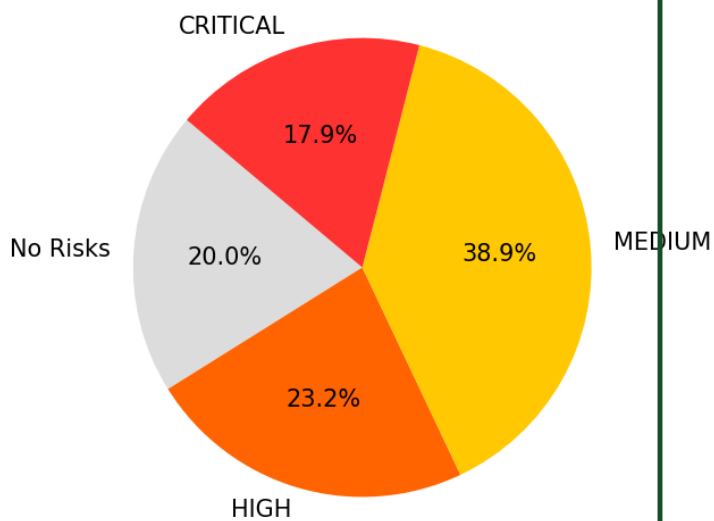
Firewall Risk Analysis Report - FireFind

Rule ID	Issue	Field	Value	Severity	Rule Category
1	No issues found	-	-	No Risks	-
2	No issues found	-	-	No Risks	-
3	No issues found	-	-	No Risks	-
4	weak_protocol	service	http	HIGH	Web
5	No issues found	-	-	No Risks	-
6	suspicious_service	service	ldap	HIGH	Web
6	suspicious_service	service	ldap	HIGH	Web
7	suspicious_service	service	smtp	HIGH	Web
7	no_logging_error	log	no log	MEDIUM	Admin
8	allow_all_service	service	all	MEDIUM	Web
8	allow_all_service	action	accept	MEDIUM	Web
9	allow_all_service	service	all	MEDIUM	Web
9	allow_all_service	action	accept	MEDIUM	Web
9	no_logging_error	log	no log	MEDIUM	Admin
10	no_logging_error	log	no log	MEDIUM	Admin
11	allow_all_service	service	all	MEDIUM	Web
11	allow_all_service	action	accept	MEDIUM	Web
12	suspicious_service	service	smtp	HIGH	Web
12	no_logging_error	log	no log	MEDIUM	Admin
13	no_logging_error	log	no log	MEDIUM	Admin
14	LPD_Port_Exposure	service	lpdw0rm	HIGH	Web
14	no_logging_error	log	no log	MEDIUM	Admin
15	No issues found	-	-	No Risks	-
16	No issues found	-	-	No Risks	-
17	allow_all_service	service	all	MEDIUM	Web
17	allow_all_service	action	accept	MEDIUM	Web
17	no_logging_error	log	no log	MEDIUM	Admin
18	No issues found	-	-	No Risks	-
19	No issues found	-	-	No Risks	-
20	no_logging_error	log	no log	MEDIUM	Admin

Firewall Risk Analysis Report - FireFind

21	no_logging_error	log	no log	MEDIUM	Admin
22	No issues found	-	-	No Risks	-
23	allow_all_service	service	all	MEDIUM	Web
23	allow_all_service	action	accept	MEDIUM	Web
24	LPD_Port_Exposure	service	lpdw0rm	HIGH	Web
24	no_logging_error	log	no log	MEDIUM	Admin
25	no_logging_error	log	no log	MEDIUM	Admin
26	No issues found	-	-	No Risks	-
27	weak_protocol	service	ftp	HIGH	Web
28	No issues found	-	-	No Risks	-
29	No issues found	-	-	No Risks	-
30	smb_netbios_exposed	service	135	CRITICAL	Web
30	smb_netbios_exposed	service	445	CRITICAL	Web
31	smb_netbios_exposed	service	135	CRITICAL	Web
31	smb_netbios_exposed	service	445	CRITICAL	Web
32	smb_netbios_exposed	service	135	CRITICAL	Web
32	smb_netbios_exposed	service	445	CRITICAL	Web
33	allow_all_service	service	all	MEDIUM	Web
33	allow_all_service	action	accept	MEDIUM	Web
34	admin_port_exposed	service	ssh	CRITICAL	Admin
34	admin_port_exposed	service	23	CRITICAL	Admin
34	weak_protocol	service	telnet	HIGH	Web
35	admin_port_exposed	service	ssh	CRITICAL	Admin
35	no_logging_error	log	no log	MEDIUM	Admin
36	admin_port_exposed	service	ssh	CRITICAL	Admin
36	admin_port_exposed	service	23	CRITICAL	Admin
36	no_logging_error	log	no log	MEDIUM	Admin
36	weak_protocol	service	telnet	HIGH	Web
37	weak_protocol	service	http	HIGH	Web
38	No issues found	-	-	No Risks	-
39	admin_port_exposed	service	23	CRITICAL	Admin

Firewall Risk Analysis Report - FireFind

39	no_logging_error	log	no log	MEDIUM	Admin
39	weak_protocol	service	telnet	HIGH	Web
40	No issues found	-	-	No Risks	-
41	allow_all_service	service	all	MEDIUM	Web
41	allow_all_service	action	accept	MEDIUM	Web
41	no_logging_error	log	no log	MEDIUM	Admin
42	No issues found	-	-	No Risks	-
43	no_logging_error	log	no log	MEDIUM	Admin
44	No issues found	-	-	No Risks	-
45	no_logging_error	log	no log	MEDIUM	Admin
45	weak_protocol	service	http	HIGH	Web
46	no_logging_error	log	no log	MEDIUM	Admin
46	weak_protocol	service	ftp	HIGH	Web
47	no_logging_error	log	no log	MEDIUM	Admin
48	weak_protocol	service	http	HIGH	Web
49	no_logging_error	log	no log	MEDIUM	Admin
50	admin_port_exposed	service	rdp	CRITICAL	Admin
50	no_logging_error	log	no log	MEDIUM	Admin
50	weak_protocol	service	http	HIGH	Web
51	weak_protocol	service	http	HIGH	Web
52	weak_protocol	service	http	HIGH	Web
53	admin_port_exposed	service	ssh	CRITICAL	Admin
53	admin_port_exposed	service	23	CRITICAL	Admin
53	admin_port_exposed	service	rdp	CRITICAL	Admin
53	no_logging_error	log	no log	MEDIUM	Admin
53	weak_protocol	service	telnet	HIGH	Web
54	no_logging_error	log	no log	MEDIUM	Admin
54	weak_protocol	service	http	HIGH	Web
55	No issues found	-	-	No Risks	-
56	No issues found	-	-	No Risks	-
57	No issues found	-	-	No Risks	-

Firewall Risk Analysis Report - FireFind

58	weak_protocol	service	http	HIGH	Web
59	weak_protocol	service	http	HIGH	Web
60	admin_port_exposed	service	ssh	CRITICAL	Admin