Firewall Risk Analysis Report - FireFind

FIREFIND RISK DETECTOR

TRISKELE LABS

Triskele Labs

Summary of the Risk Analysis

Metric	Value
File Analyzed	Sophos-XG-2.csv
File Belongs to	Sophos
Total Rules Analyzed	20
Total Risks Found	25
No Risks	10
High Risks	19
Medium Risks	4
Critical Risks	2
Analyzed Date and Time	2025-10-14 17:04:26

Risks by Severity

MEDIUM

CRITICAL

11.4%

5.7%

No Risks

28.6%

54.3%

HIGH

Risks by Category
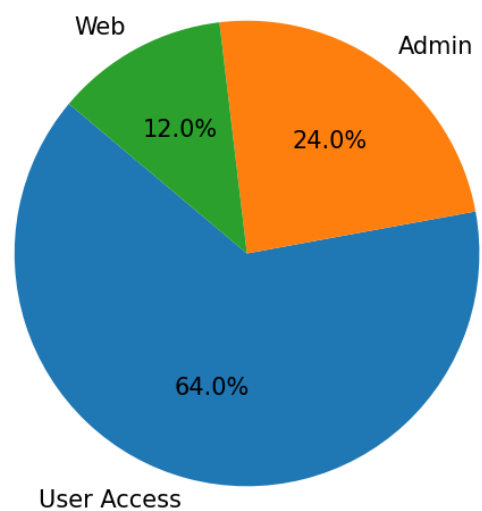
Web

Admin

12.0%

24.0%

64.0%
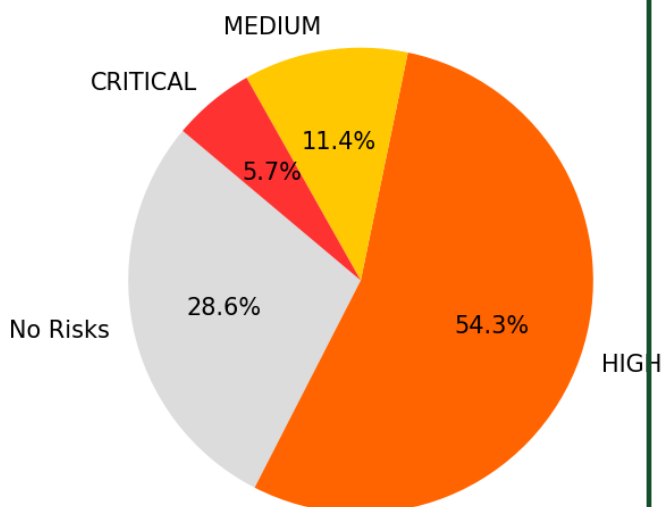
User Access

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	allow_all_destination_port	dstaddr	any	HIGH	User Access
3	allow_all_destination_port	action	allow	HIGH	User Access
4	allow_all_destination_port	dstaddr	any	HIGH	User Access
4	allow_all_destination_port	action	allow	HIGH	User Access
4	no_logging_error	log	disable	MEDIUM	Admin
5	allow_all_destination_port	dstaddr	any	HIGH	User Access
5	allow_all_destination_port	action	allow	HIGH	User Access
5	weak_protocol	service	http	HIGH	Web
6	allow_all_destination_port	dstaddr	any	HIGH	User Access
6	allow_all_destination_port	action	allow	HIGH	User Access
7	No issues found	-	-	No Risks	-
8	allow_all_destination_port	dstaddr	any	HIGH	User Access
8	allow_all_destination_port	action	allow	HIGH	User Access
8	no_logging_error	log	disable	MEDIUM	Admin
8	weak_protocol	service	http	HIGH	Web
9	allow_all_destination_port	dstaddr	any	HIGH	User Access
9	allow_all_destination_port	action	allow	HIGH	User Access
9	no_logging_error	log	disable	MEDIUM	Admin
10	No issues found	-	-	No Risks	-
11	No issues found	-	-	No Risks	-
12	admin_port_exposed	service	ssh	CRITICAL	Admin
13	admin_port_exposed	service	rdp	CRITICAL	Admin
14	allow_all_destination_port	dstaddr	any	HIGH	User Access
14	allow_all_destination_port	action	allow	HIGH	User Access
14	suspicious_service	service	smtp	HIGH	Web
15	No issues found	-	-	No Risks	-
16	No issues found	-	-	No Risks	-
17	allow_all_destination_port	dstaddr	any	HIGH	User Access

Firewall Risk Analysis Report - FireFind

17	allow_all_destination_port	action	allow	HIGH	User Access
17	no_logging_error	log	disable	MEDIUM	Admin
18	No issues found	-	-	No Risks	-
19	No issues found	-	-	No Risks	-
20	No issues found	-	-	No Risks	-