Firewall Risk Analysis Report - FireFind

Summary of the Risk Analysis

Metric	Value
File Analyzed	Sophos-XG-1.csv
File Belongs to	Sophos
Total Rules Analyzed	20
Total Risks Found	21
High Risks	12
No Risks	10
Medium Risks	5
Critical Risks	4
Analyzed Date and Time	2025-10-03 10:34:36

Severity Distribution

CRITICAL 12.9%
MEDIUM 16.1%
No Risks 32.3%
HIGH 38.7%
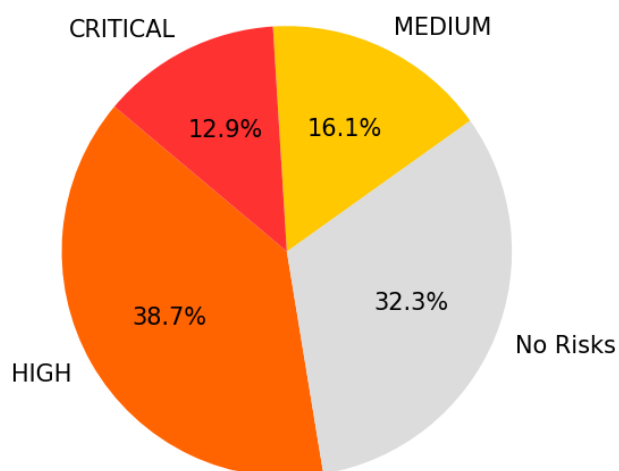
Rule Category Distribution

Admin 23.8%
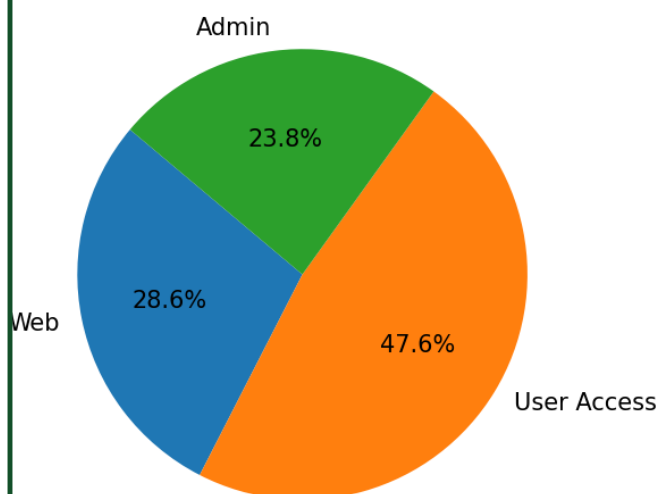Web 28.6%
User Access 47.6%

Firewall Risk Analysis Report - FireFind

Rule ID	Issue	Field	Value	Severity	Rule Category
1	weak_protocol	service	http	HIGH	Web
2	No issues found	-	-	No Risks	-
3	No issues found	-	-	No Risks	-
4	allow_all_destination_port	dstaddr	any	HIGH	User Access
4	allow_all_destination_port	action	allow	HIGH	User Access
4	allow_all_service	service	any	MEDIUM	Web
4	allow_all_service	action	allow	MEDIUM	Web
5	No issues found	-	-	No Risks	-
6	allow_all_destination_port	dstaddr	any	HIGH	User Access
6	allow_all_destination_port	action	allow	HIGH	User Access
7	allow_all_destination_port	dstaddr	any	HIGH	User Access
7	allow_all_destination_port	action	allow	HIGH	User Access
7	no_logging_error	log	disable	MEDIUM	Admin
8	admin_port_exposed	service	ssh	CRITICAL	Admin
9	admin_port_exposed	service	rdp	CRITICAL	Admin
10	No issues found	-	-	No Risks	-
11	No issues found	-	-	No Risks	-
12	allow_all_destination_port	dstaddr	any	HIGH	User Access
12	allow_all_destination_port	action	allow	HIGH	User Access
12	suspicious_service	service	smtp	HIGH	Web
13	allow_all_destination_port	dstaddr	any	HIGH	User Access
13	allow_all_destination_port	action	allow	HIGH	User Access
13	allow_all_service	service	any	MEDIUM	Web
13	allow_all_service	action	allow	MEDIUM	Web
14	No issues found	-	-	No Risks	-
15	admin_port_exposed	service	ssh	CRITICAL	Admin
16	No issues found	-	-	No Risks	-
17	No issues found	-	-	No Risks	-
18	admin_port_exposed	service	rdp	CRITICAL	Admin
19	No issues found	-	-	No Risks	-

Firewall Risk Analysis Report - FireFind

20	No issues found	-	-	No Risks	-