FireFind Security Report

Generated on: 2025-10-25 16:18:12

Security Findings Summary

Total Findings: 35

Critical: 1

High: 2

Low: 17

Medium: 15

Rule ID	Title	Source	Destination	Service	Severity	Vendor
10025	Very wide service port span	location_SRA_INT, SRA_EXT	Direction-Location-LAN, [Network]	any	Medium	Sophos
10031	Very wide service port span	Direction-Location-LAN, [Network]	system_10.80.100.0	any	Medium	Sophos
10044	Very wide service port span	System3_172.16.1.1	Direction-Location-LAN, [Network]	any	Medium	Sophos
10045	Very wide service port span	REF_NetDnsLanLocation a,rra REF_NetDnsLanLocation a2ra REF_NetDnsLanLocation a3ra REF_NetDnsLanLocation a3ra REF_NetDnsLanLocation a5ra	DMZ_2_192.168.2.123	any	Medium	Sophos
10023	Admin ports exposed to/from internet-like	Monitoring_172.16.0.1	any	udp/137, tcdp/2138, tcp/139, tcp/445, tcp/5986, icmp	Critical	Sophos
10023	Windows admin services exposed	Monitoring_172.16.0.1	any	udp/137, tcdp/2138, tcp/139, tcp/445, tcp/5986, icmp	High	Sophos

FireFind Security Report

Generated on: 2025-10-25 16:18:12

Rule ID	Title	Source	Destination	Service	Severity	Vendor
10023	SSH broadly allowed	Monitoring_172.16.0.1	any	udp/137, udp/138, tcp/22, tcp/139, tcp/445, tcp/5985, tcp/5986, icmp	Medium	Sophos
10023	ICMP broadly allowed	Monitoring_172.16.0.1	any	udp/137, udp/138, tcp/22, tcp/139, tcp/445, tcp/5985, tcp/5986, icmp	Low	Sophos
10026	HTTP allowed (80/tcp)	location_WLAN-Staff, location_LAN	Direction-Location-LAN, [Network]	tcp/80, tcp/88, tcp/389, tcp/443, tcp/445, tcp/636, udp/88, udp/123	Low	Sophos
10019	HTTP allowed (80/tcp)	Direction-Location-LAN, [Network]	Internet IPv4 Internet IPv6	tcp/22, tcp/80, tcp/443	Low	Sophos
10015	Very wide service port span	LAN_10.1.100.100	Direction-Location-LAN, [Network] Direction-Location-Mgmt-ESX [Network]	any	Medium	Sophos
10012	Very wide service port span	location_LAN, Direction-Location-LAN [Network]	location_LAN, Direction-Location-LAN [Network]	any	Medium	Sophos
10001	Very wide service port span	LAN_10.1.1.170	any	any	Medium	Sophos
10016	Very wide service port span	GRP_Nadmin-Access	Direction-Location-IP-WAN [Network] Direction-Location-LAN [Network] Direction-Location-Mgmt-ESX [Network] Direction-Location-Voice [Network]	any	Medium	Sophos

FireFind Security Report

Generated on: 2025-10-25 16:18:12

Rule ID	Title	Source	Destination	Service	Severity	Vendor
10018	Very wide service port span	NDC_VPN-Pool-SSL	Direction-Location-IP-WA N [Network] Direction-Location-LAN [Network] Direction-Location-Mgmt- ESX [Network] Direction-Location-Voice [Network]	any	Medium	Sophos
10035	Very wide service port span	NDC-Voice, Direction-Location-Voice [Network]	NDC-Voice, Direction-Location-Voice [Network]	any	Medium	Sophos
10004	HTTP allowed (80/tcp)	any	REF_NetDnsWanauboots ,REF_NetDnsWanaudatai REF_NetDnsWanaudeplo REF_NetDnsWanauendp cREF_NetDnsWanaustora REF_NetDnsWancrlsca1	tcp/80, tcp/443	Low	Sophos
10004	HTTP exposed to/from internet-like	any	REF_NetDnsWanauboots ,REF_NetDnsWanaudatai REF_NetDnsWanaudeplo REF_NetDnsWanauendp cREF_NetDnsWanaustora REF_NetDnsWancrlsca1	tcp/80, tcp/443	Medium	Sophos
10005	HTTP allowed (80/tcp)	any	REF_NetDnsWancontent, REF_NetDnsWancrlgoda REF_NetDnsWandev5con REF_NetDnsWandevices REF_NetDnsWandevprod REF_NetDnsWandevprod 2REF_NetDnsWandevprod 3REF_NetDnsWanoscpgod REF_NetDnsWanupdates	tcp/80, tcp/443, tcp/54443	Low	Sophos

FireFind Security Report

Generated on: 2025-10-25 16:18:12

Rule ID	Title	Source	Destination	Service	Severity	Vendor
10005	HTTP exposed to/from internet-like	any	REF_NetDnsWancontent, REF_NetDnsWancrlgoda REF_NetDnsWandev5con REF_NetDnsWandevices REF_NetDnsWandevprod REF_NetDnsWandevprod 2REF_NetDnsWandevprod 3REF_NetDnsWanoscpgod REF_NetDnsWanupdates	tcp/80, tcp/443, tcp/54443	Medium	Sophos

FireFind Security Report

Generated on: 2025-10-25 16:18:12

Rule ID	Title	Source	Destination	Service	Severity	Vendor
10007	HTTP allowed (80/tcp)	Private-Range-A_10.0.0.0 /8, Private-Range-B_172.16. 0.0/ 12 Private-Range-C_192.168 .0.0 /16	REF_NetDnsWanactivat, REF_NetDnsWanadlwind REF_NetDnsWanclientw REF_NetDnsWancrlmicr REF_NetDnsWandownloa REF_NetDnsWandownloa 3 REF_NetDnsWandsdownl REF_NetDnsWanemdlws m REF_NetDnsWanfe2crup REF_NetDnsWanfe2crup 2 REF_NetDnsWanfe2upda REF_NetDnsWanfe2wsmi REF_NetDnsWanfsmicro REF_NetDnsWangomicro REF_NetDnsWanlocation next REF_NetDnsWanmicroso REF_NetDnsWanmspana b REF_NetDnsWanntservi REF_NetDnsWanocspdig REF_NetDnsWansetting REF_NetDnsWansg2pwn s REF_NetDnsWansisnabl REF_NetDnsWanslsmicr REF_NetDnsWanslsupda REF_NetDnsWansmicros REF_NetDnsWanLocation d ext REF_NetDnsWantsetsta REF_NetDnsWanupdate m REF_NetDnsWanwindow s REF_NetDnsWanwindow s2 REF_NetDnsWanwindow s3 REF_NetDnsWanwwwmic r	tcp/80, tcp/443	Low	Sophos

FireFind Security Report

Generated on: 2025-10-25 16:18:12

Rule ID	Title	Source	Destination	Service	Severity	Vendor
10010	HTTP allowed (80/tcp)	Direction-Location-LAN, [Network] Direction-Location-Mgmt-ESX [Network]	LAN_10.1.1.38	tcp/80, tcp/443	Low	Sophos
10011	HTTP allowed (80/tcp)	Direction-Location-LAN, [Network]	Hosting-Access_192.168.250.130, Hosting-Access_192.168.250.140. GRP_BCCePermWebPrivate GRP_Hosting_Web location_DMZ_WEB SRA_EXT_192.168.8.30 SRA_EXT_192.168.8.40 SRA_INT_192.168.12.30 SRA_INT_192.168.12.40	tcp/80, tcp/443	Low	Sophos
10013	Very wide service port span	Direction-Location-LAN, [Network]	Internet IPv4 Internet IPv6	any	Medium	Sophos
10020	Insecure clear-text protocols allowed broadly	Monitoring_172.16.0.100, Monitoring_172.16.0.50 Monitoring_172.16.0.70	any	udp/161, icmp	High	Sophos
10020	ICMP broadly allowed	Monitoring_172.16.0.100, Monitoring_172.16.0.50 Monitoring_172.16.0.70	any	udp/161, icmp	Low	Sophos
10021	HTTP allowed (80/tcp)	Direction-Location-Mgmt-ESX, [Network]	Monitoring_172.16.0.80, Monitoring_172.16.0.120	tcp/80, tcp/443, udp/6559	Low	Sophos
10022	HTTP allowed (80/tcp)	Direction-Location-LAN, [Network] Direction-Location-Mgmt-ESX [Network]	Monitoring_172.16.0.100	tcp/80, tcp/4505-4506	Low	Sophos
10024	HTTP allowed (80/tcp)	Direction-Location-LAN, [Network]	DMZ_WEB_192.168.11.200	tcp/80, tcp/443	Low	Sophos

FireFind Security Report

Generated on: 2025-10-25 16:18:12

Rule ID	Title	Source	Destination	Service	Severity	Vendor
10027	Very wide service port span	Direction-Location-LAN, [Network]	Hosting-Access_192.168. 250. 14	any	Medium	Sophos
10028	HTTP allowed (80/tcp)	Direction-Location-LAN, [Network]	system_SDE-Portal, system_locationtscxsp01. enet syst	tcp/80, tcp/443	Low	Sophos
10029	HTTP allowed (80/tcp)	Direction-Location-LAN, [Network]	system_10.80.118.0, system_Storefront715.sys tem ten	tcp/80, tcp/443, tcp/2598, udp/16500-1650 2598,	Low	Sophos
10038	HTTP allowed (80/tcp)	Direction-Location-LAN, [Network]	Exchange-location_EXDA 01 Location.client2.com.au, Exchange-location_EXDA 02 Location.client2.com.au	9 tcp/80, tcp/443	Low	Sophos
10040	HTTP allowed (80/tcp)	Direction-Location-LAN, [Network]	Citrix_192.168.120.52	tcp/80, tcp/443	Low	Sophos
10042	HTTP allowed (80/tcp)	LAN_LocationARRA-3952 em client2.com.au, LAN_LocationARRA-3962 em client2.com.au location_LAN REF_NetDnsLanLocation 33 ara Direction-Location-LAN [Network]	DMZ_2_192.168.2.122, DMZ_2_192.168.2.123	tcp/80, tcp/3007-3008, tcp/8006-8007, tcp/30175	Low	Sophos