



ISO

ISO 27001 Firewall Audit Report

11/10/2023

Table of Contents

Table of Contents	2
ISO 27001 Firewall Audit Report Executive Summary	3
Logging Status of The System	4
Risky Service Usage on Rules	6
Usage of The Rules on Firewalls	10
Shadow Status of Rules	11
Expiry Status of The Rules	18
Permissive Rule Usage on Firewalls	20
Software Version Status	25
Corporate Security Policy Compliance	26
Existing Firewall Topology	28
Comment Usage on The Rules	29
Admin Users on The System	31

ISO 27001 Firewall Audit Report Executive Summary

The ISO27001 firewall audit report provides an assessment of the effectiveness of the firewall implementation in place within the organization against the ISO27001 standard. The audit aimed to identify any weaknesses, vulnerabilities, and gaps in the current firewall setup and provide recommendations for improvement.


This report presents a list of audit items and the current situation of the company with respect to each item. The report aims to provide information about the audit items to facilitate the audit process, and it does not pass judgment on the company's compliance level. The contents of this report are intended for the use of audit teams as a reference during their audit.

In the first part of the report overall status of the environment be given with topology, device information and a summary of some statistical values. Afterwards, detailed information be given on the remaining aspects of the environment.

Logging Status of The System

Logging must be enabled on each rule for compliancy. Here is the list of first 20 rules on each firewall that are not logged.

Logging Disabled Rules	459
Total Rules	1217

 cp_cluster | cp-cluster # Logging Disabled Rules: 2 | Total Rules: 12


Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
12	any	any	any	N/A	any	any	any		always	deny	Enabled
11	any	any	any	N/A	cp-gateway1 cp-cluster	any	any		always	accept	Enabled

 FG_Opinstate_1 # Logging Disabled Rules: 1 | Total Rules: 453


Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
576	any	any	any	N/A	185.67.34.90/32 *.usom.gov.tr	HTTP HTTPS	N/A		always	accept	Enabled

 FG_Opinstate_2 | Customer_vd # Logging Disabled Rules: 2 | Total Rules: 96

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
2	port6	vlan_112A°	50.50.50.50/32	N/A	autoupdate.opera.com	HTTP HTTPS	N/A		always	accept	Enabled
7	port6	vlan_112A°	any	N/A	any	any	N/A		always	deny	Enabled

 Palo_Alto_1 # Logging Disabled Rules: 369 | Total Rules: 386

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
ipsec	any	any	10.34.128.201 10.34.128.203	N/A	10.34.128.201 10.34.128.203	any	any		always	accept	Enabled
Jupiter Int Erisimi	test_ui	untrust	JUPITER01-172.22.3.177 JUPITER02-172.22.3.178	N/A	134.170.94.0/24 185.152.252.0/22 204.79.197.0/24 216.58.209.0/24 maps-172.217.16.0 maps-172.217.18.0 maps-172.217.20.0 maps.googleapis.com	service-http service-https	any	OP-431	always	accept	Disabled
EDL Deny List	test_ui test_db test_app	untrust	any	N/A	192.168.30.30_31 192.168.40.4-192.168.40.20 192.168.50.5_32	service-http service-https	any	dstcck3	always	deny	Enabled
usom2	test_db	test_ui	fortiguard usom	N/A	192.168.132.150_32 192.168.133.10-192.168.133.50	tcp_10	any	OP-1	always	accept	Enabled
OP-1-2	test_db	test_ui	usom 192.147.15.26_32	N/A	192.168.30.30_31 192.168.40.4-192.168.40.20 192.168.50.5_32 192.147.15.26_32	tcp_10	any	OP-1-dstcck3-OP-5666	always	accept	Enabled
OP-1	test_db	test_ui	192.168.140.50_32	N/A	192.168.133.10-192.168.133.50 192.168.132.150_32	tcp_10	any	OP-1	always	accept	Enabled
OP-40	any	any	vip-asa-10.34.128.189 192.168.140.50_32 55.55.55.55_32	N/A	6.6.6.6_32 192.168.140.50_32 192.168.132.150_32 89.89.89.89_32	tcp_56 udp_65 tcp_89 udp_33 tcp_333	any	OP-4576Hahahahaha-OP-141-OP...	always	accept	Enabled
usom2-1	test_db	test_ui	AZ CU	N/A	192.168.132.150_32 192.168.133.10-192.168.133.50	tcp_10	any	anil2anil3-OP-137	always	accept	Enabled
OP-190	any	any	155.155.155.155_32	N/A	166.166.166.166_32	tcp_155 udp_166	any	OP-190	always	accept	Enabled
OP-190-1	any	any	166.166.166.166_32	N/A	155.155.155.155_32	tcp_155 udp_166	any	OP-190	always	accept	Enabled
OP-295	test_ui	untrust	192.168.133.125_32	N/A	192.168.50.73_32	tcp_8090	any	OP-295	always	accept	Enabled
OP-295-3	untrust	test_db	192.168.50.73_32	N/A	192.168.133.121_32 192.168.140.53_32	tcp_2431 udp_56 udp_99 tcp_123	any	OP-295-3-OP-57-OP-5276	always	accept	Enabled
OP-295-3-i	untrust	test_db	192.168.50.73_32	N/A	192.168.133.121_32 192.168.140.53_32	any	icmp	OP-295-3-OP-57-OP-5276	always	accept	Enabled
OP-295-5	untrust	test_db	192.168.50.73_32	N/A	192.168.140.73_32	tcp_443 tcp_445	any	OP-295-5	always	accept	Enabled
OP-295-6	test_db	untrust	192.168.140.73_32	N/A	192.168.50.73_32	tcp_443 tcp_445	any	OP-295-6	always	accept	Enabled
OP-295-7	untrust	test_ui	192.168.50.73_32	N/A	192.168.133.126_32	tcp_312 udp_89	any	OP-295-7	always	accept	Enabled
OP-295-7-i	untrust	test_ui	192.168.50.73_32	N/A	192.168.133.126_32	any	icmp	OP-295-7	always	accept	Enabled
OP-306	untrust	test_db	192.168.83.20_32 192.168.73.20_32	N/A	192.168.140.20_32	tcp_443 tcp_4456	any	OP-306-OP-330-OP-343-OP-466...	always	accept	Enabled
OP-351	untrust	test_db	192.168.83.25_32 192.168.73.25_32	N/A	192.168.140.25_32	tcp_25	any	OP-351-OP-362-OP-389-OP-410	2023_08_16T00_00	accept	Enabled
OP-352	untrust	test_db	192.168.50.25_32	N/A	192.168.140.25_32	tcp_25	any	OP-352	2023_08_16T00_00	accept	Enabled


 FG_Opinstate_2 | root # Logging Disabled Rules: 2 | Total Rules: 167

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
18	port1 cp_net port2	cp_net port1	10.0.0.110 10.0.0.111 178.157.15.222/32	N/A	10.0.0.110 10.0.0.111 178.157.15.222/32	any	N/A	OP-59	always	accept	Enabled
52	any	any	any	N/A	185.67.34.90 usom.gov.tr	any	N/A		always	accept	Enabled


 PaloAlto_2 # Logging Disabled Rules: 66 | Total Rules: 66

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
OP-1	external	prod_db	192.168.140.50_32 192.168.30.30_32	N/A	192.168.132.150_32	tcp_10	any	anil2-OP-5000	always	accept	Enabled
usom-1	any	any	fortiguard usom	N/A	2.2.2.2_32 8.8.8.8_32	tcp_12 tcp_21 tcp_89 tcp_98 udp_89 udp_98	any	Opinnate131testOP-483	2023_07_22T00_00	accept	Enabled

usom	any	any	usom	N/A	2.2.2.2_32	tcp_12 tcp_21 tcp_89 tcp_98 udp_89 udp_98	any	Opinnate131testanii30P-46-O...	always	accept	Enabled
OP-17-1	any	any	9.9.9.9_32	N/A	2.2.2.2_32	tcp_89 tcp_98 udp_89 udp_98 tcp_12 tcp_21	any	a1b2anii3-CANCAN-OP-254	2023_07_22T00_00	accept	Enabled
OP-40	any	any	5.5.5.5_32 9.19.19.19_32 91.91.91.91_32 4.6.7.6_32 192.160.30.68_32 55.55.55.55_32	N/A	9.19.19.19_32 91.91.91.91_32 6.6.6.6_32	tcp_56 udp_65	any	a1b2test1-CANCAN-OP-151-OP...	always	accept	Enabled
OP-40-1	any	any	6.6.6.6_32 91.91.91.91_32 1.3.3.3_32 1.3.2.4_32	N/A	5.5.5.5_32 9.19.19.19_32 91.91.91.91_32 55.55.55.55_32	tcp_56 udp_65	any	OP-40-anilc2opinnate1-CAN-C...	always	accept	Enabled
OP-80	any	any	192.168.10.10_32 192.168.10.11_32 1.3.3.3_32 1.3.2.4_32 9.9.99.9_32	N/A	192.168.20.21_32	tcp_443	any	OP-80-CAN-OP-186-OP-4633-OP...	always	accept	Enabled
OP-190	any	any	155.155.155.155_32	N/A	166.166.166.166_32	tcp_155 udp_166	any	OP-190	always	accept	Enabled
OP-190-1	any	any	166.166.166.166_32 1.4.5.7_32	N/A	155.155.155.155_32	tcp_155 udp_166	any	OP-190-OP-4994	always	accept	Enabled
OP-295	prod_app	external	192.168.52.0_24 192.168.30.69_32	N/A	192.168.50.73_32	tcp_80	any	OP-295-OP-5005	always	accept	Enabled
OP-295-3	external	prod_db	192.168.50.73_32	N/A	192.168.132.188_32	tcp_2431 udp_56 udp_99 tcp_123	any	OP-295-3-revpolidyupdaOP-49...	always	accept	Enabled
OP-295-3-i	external	prod_db	192.168.50.73_32	N/A	192.168.132.188_32 192.168.132.181_32	any	icmp	revreplaceComment	always	accept	Enabled
OP-295-5-i	external	prod_db	192.168.50.73_32	N/A	192.168.132.169_32	any	icmp	aas	always	accept	Enabled
OP-524	external	prod_db	192.168.40.40_32	N/A	192.168.132.137_32	tcp_555	any	OP-524OP-529OP-531	2023_08_30T00_00	accept	Enabled
OP-5029	any	any	192.168.10.25_32	N/A	192.168.30.55_32	tcp_32	any	OP-5029	always	accept	Enabled
OP-659	any	any	5.5.5.5_32	N/A	6.6.6.6_32	tcp_80 tcp_81	any	OP-659	2023_09_10T00_00	accept	Disabled
commen-Policy	external	prod_db	192.168.170.15_32 192.168.170.16_32	N/A	192.168.180.17_32	tcp_58 udp_62	any	commen-Policy-OP-32-OP-5244...	always	accept	Enabled
commen-Policy-i	external	prod_db	192.168.170.15_32 192.168.170.16_32 192.168.170.24_32	N/A	192.168.180.17_32	any	icmp	commen-Policy-OP-32	always	accept	Enabled
OP-43	external	prod_db	192.168.12.44_32	N/A	192.168.132.174_32	tcp_80 tcp_443 tcp_3125-5588	any	OP-43	always	accept	Enabled
OP-51	prod_db prod_app	external	any	N/A	192.168.150.17_32 192.168.170.55_32 192.168.133.14_32	tcp_99-195 tcp_66 udp_73	any	OP-51	always	accept	Enabled

 cp-2sms | vs_3rd_party

No Data

 cp-sms2 | vs_opinnate


No Data

 cp-sms1 | cp-node # Logging Disabled Rules: 1 | Total Rules: 9

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
9	any	any	any	N/A	any	any	any		always	deny	Enabled

 PA3000-OP3 # Logging Disabled Rules: 16 | Total Rules: 28

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
cp-sms-spark	cp_spark_zone fg1_zone	cp_spark_zone fg1_zone	10.0.0.110 cp-192.168.160.1	N/A	10.0.0.110 cp-192.168.160.1	any	any		always	accept	Enabled
cp-spark-erisim	untrust	any	op-net-10.34.128.0_23	N/A	any	any	any	OP-288OP-289	always	accept	Enabled
OP-5610	any	any	172.16.25.14_32	N/A	172.49.58.56_32	tcp_50 tcp_423 tcp_41	any	OP-5610	always	accept	Enabled
OP-379	untrust	cp_spark_zone	192.168.120.55_32 192.168.120.56_32 1.1.1.1_32	N/A	192.168.160.3_32 192.168.160.4_32 1.1.1.1_32	tcp_444 tcp_445 udp_445	any	OP-379-OP-490-OP-491-OP-492...	always	accept	Enabled
OP-5680	any	any	213.12.42.55_32 213.12.42.54_32	N/A	44.32.11.45_32	tcp_44 tcp_553	any	OP-5680-OP-483	always	accept	Enabled
OP-458	untrust cp_spark_zone	untrust	any	N/A	172.145.21.3_32 172.35.68.69_32	tcp_445	any	test	always	accept	Enabled
OP-458-1	untrust cp_spark_zone	untrust fg1_zone	any	N/A	172.168.36.23_32 192.168.133.9-192.168.133.49 172.35.68.69_32	tcp_66 tcp_42 tcp_21 tcp_43	any	testupdate	always	accept	Enabled
OP-569	any	any	157.157.157.157_32	N/A	158.158.158.158_32	tcp_157 tcp_158	any	OP-569	always	accept	Enabled
OP-694	any	any	8.8.8.8_32	N/A	9.9.9.9_32	tcp_443	any	OP-694	always	accept	Enabled
OP-667	untrust	cp_spark_zone	192.168.120.100_32 3.3.3.3_32 4.4.4.4_32	N/A	192.168.160.3_32	tcp_444	any	OP-667-OP-6875-OP-6877disable	always	accept	Enabled
OP-5883	untrust	cp_spark_zone	192.168.120.10_32 192.168.120.11_32 192.168.12.11_32	N/A	192.168.160.3_32	tcp_444	any	OP-5883disable-OP-5910-OP-5908	always	accept	Enabled
OP-5903	untrust	cp_spark_zone	192.168.120.10_32	N/A	192.168.160.3_32	tcp_444	any	OP-5903	always	accept	Enabled
OP-5918	untrust	cp_spark_zone	192.168.120.100_32	N/A	192.168.160.3_32	tcp_444	any	OP-5918	always	accept	Enabled
OP-5936	untrust	cp_spark_zone	10.0.0.10_32	N/A	192.168.160.3_32	tcp_444 tcp_443	any	OP-5936-OP-5970	always	accept	Enabled
OP-5975	fg1_zone	cp_spark_zone untrust	192.168.140.10_32	N/A	192.168.160.3_32 any	tcp_444	any	OP-5975	always	accept	Enabled
OP-5976	any	any	192.168.133.10_32	N/A	192.168.83.86_32	tcp_3389	any	OP-5976	2023_11_09T00_00	accept	Enabled

 PA-Opinnate-v9

No Data

Risky Service Usage on Rules

There must be no rules containing risky service allowance. Here is the list of first 20 rules on each firewall that are using risky services.

Rules on Risky Services or Protocols	463
Total Rules	1217



cp_cluster | cp-cluster # Rules on Risky Services or Protocols: 10 | Total Rules: 12

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
11	any	any	any	N/A	cp-gateway1 cp-cluster	any	any		always	accept	Enabled
10	any	any	192.168.133.10	N/A	192.168.83.86	Tcp_3389	any	OP-5976	091123T0000	accept	Enabled
9	any	any	5.54.54.3	N/A	78.78.8.8	Tcp_3389	any	OP-5977	always	accept	Enabled
8	any	any	3.56.6.3	N/A	4.1.55.4	Tcp_3389	any	OP-5978	always	accept	Enabled
7	any	any	9.9.9.9	N/A	10.10.10.10	Tcp_3389	any	OP-5979	always	accept	Enabled
6	any	any	6.6.6.6	N/A	77.7.7.7	Tcp_3389	any	OP-5980	always	accept	Enabled
5	any	any	5.5.5.5	N/A	5.5.5.56	Tcp_3389 tcp_3389	any	OP-5985	always	accept	Enabled
4	any	any	44.5.6.6	N/A	9.8.7.21	tcp_445	any	OP-5986	always	accept	Enabled
3	any	any	13.15.16.16	N/A	.test.com 8.8.8.6	tcp_445	any	OP-5982	always	accept	Enabled
2	any	any	10.0.0.100	N/A	10.115.207.100	Tcp_3389 tcp_3389	any	OP-5995	101123T0000	accept	Enabled



FG_Opinnte_1 # Rules on Risky Services or Protocols: 154 | Total Rules: 453


Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
576	any	any	any	N/A	185.67.34.90/32 *.usom.gov.tr	HTTP HTTPS	N/A		always	accept	Enabled
1	any	any	https_eriÅim_grp	N/A	any	HTTPS SSH	N/A	OP-58	always	accept	Enabled
611	any	any	10.34.128.0/23	N/A	10.0.0.0/8	any	N/A	OP-58Copyofhttps	always	accept	Enabled
4	any	any	192.168.8.70/32 192.168.9.71-192.168.9.103	N/A	192.168.13.8/32	tcp_99-195 tcp_66 ALL_ICMP udp_73 NFS	N/A		always	accept	Enabled
11	any	any	client 0/8_network 127.0.0.0/8	N/A	forti_4 172.16.0.0/12 192.168.0.0/16	tcp_80 ALL_ICMP	N/A		always	accept	Enabled
25	any	any	Deneme_grp_1	N/A	192.168.50.11/32 192.168.50.100/32 192.168.50.17/32 192.168.50.12/32	udp_53	N/A	grpaccess1OP-2539	always	accept	Enabled
29	sd-wan2	sd-wan3	192.168.20.20/32 192.168.20.21/32	N/A	192.168.132.132/32	tcp_22	N/A	OP-4083	always	accept	Enabled
33	any	any	192.168.13.8/32	N/A	192.168.8.70/32 192.168.9.71-192.168.9.103	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A		always	accept	Enabled
55	any	any	192.168.8.70/32 192.168.9.71-192.168.9.103	ldap_grp admanil CN=10b3ad2a-6883-4fa7-90...	192.168.13.8/32	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A		always	accept	Enabled
109	any	any	A_group_1	N/A	B_grp_2	udp_11	N/A	CopyofOP-868	always	accept	Enabled
82	any	any	A_group_1	CN=293f0798-aa5c-4455-9f...	B_grp_2	udp_11	N/A		always	accept	Enabled
83	any	any	A_group_1 192.168.13.8/32	N/A	B_grp_2	tcp_11	N/A		always	accept	Enabled
84	any	any	A_grp	N/A	X_grp	tcp_443 tcp_79 udp_79	N/A		always	accept	Enabled
85	any	any	A_group_1	N/A	B_grp_2	tcp_443 tcp_79 udp_79	N/A		always	accept	Enabled
98	any	any	any	oplocal\admalitest oplocal\admanil	192.168.13.8/32	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A		always	accept	Enabled
101	any	any	192.168.8.70/32 192.168.9.71-192.168.9.103	oplocal\admmert oplocal\admanil	192.168.13.8/32	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A	SNSA-55	always	accept	Enabled
105	any	any	192.168.8.70/32 192.168.9.71-192.168.9.103	oplocal\admmert	192.168.112.0/24	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A	SNSA-55	always	accept	Enabled
103	any	any	192.168.8.70/32 192.168.9.71-192.168.9.103	oplocal\admmert	192.168.13.8/32	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A	SNSA-55	always	accept	Enabled
120	any	any	host_75.75.75.75 192.168.25.97/32	N/A	192.168.30.50/32	udp_53	N/A	OP-2OP2OP-2OP-2OP-2OP-2...	always	accept	Enabled
133	any	any	192.168.50.50/32	N/A	192.168.132.142/32	any	N/A	1641	always	accept	Enabled



FG_Opinnte_2 | Customer_vd # Rules on Risky Services or Protocols: 19 | Total Rules: 96

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
2	port6	vlan_112A*	50.50.50.50/32	N/A	autoupdate.opera.com	HTTP HTTPS	N/A		always	accept	Enabled
25	any	any	Mobile-app	N/A	Database-grp	tcp_443 tcp_80	N/A	OP-61	always	accept	Enabled
33	vdom_link11	vlan_112A*	192.168.73.73/32	N/A	192.168.112.0/24	any	N/A	OP-84	always	accept	Enabled
69	vlan_112A* vdom_link11	vdom_link11 vlan_112A*	192.168.112.50/32 1.3.3.3/32 192.168.99.50/32	N/A	192.168.50.50/32 192.168.30.30/32 1.3.3.3/32 192.168.99.50/32 192.168.112.50/32	any	N/A	OP-4342	always	accept	Enabled
68	vlan_112A* vdom_link11	vdom_link11 vlan_112A*	192.168.112.50/32 192.168.99.50/32	N/A	192.168.50.50/32 192.168.30.30/32 192.168.99.50/32 192.168.112.50/32	any	N/A	OP-4342	always	accept	Enabled
65	vdom_link11	vlan_112A*	192.168.99.50/32	N/A	192.168.112.68/32	udp_3	N/A	OP-4342	always	accept	Enabled
62	vlan_112A*	vdom_link11	192.168.112.50/32 192.168.112.36/32 192.168.112.85/32 192.168.112.92/32 192.168.112.53/32 192.168.112.126/32	N/A	192.168.99.50/32	any	N/A	OP-4342	always	accept	Enabled
61	vdom_link11	vlan_112A*	192.168.99.50/32	N/A	192.168.112.58/32 192.168.112.112/32	any	N/A	OP-4342	always	accept	Enabled
48	vdom_link11	vlan_112A*	192.168.83.222/32 192.168.140.222/32	N/A	192.168.112.222/32	tcp_443 tcp_80	N/A	OP-113	2023_06_30T00:00	accept	Enabled

49	vdom_link11	vlan_112A°	192.168.30.222/32	N/A	192.168.112.222/32	tcp_443 tcp_80	N/A	differentcomment	2023_06_30T00:00	accept	Enabled
72	vdom_link11	vlan_112A°	192.168.140.22/32	N/A	192.168.112.22/32	tcp_22 tcp_443	N/A	OP-32	2023_07_27T00:00	accept	Enabled
79	vdom_link11	vlan_112A°	192.168.140.25/32	N/A	192.168.112.25/32	tcp_443 tcp_80	N/A	OP-41	always	accept	Enabled
81	vdom_link11	vlan_112A°	192.168.50.25/32	N/A	192.168.112.25/32	tcp_443 tcp_80	N/A	OP-42	always	accept	Enabled
84	vdom_link11	vlan_112A°	192.168.140.11/32	N/A	192.168.112.11/32	tcp_443 tcp_80	N/A	OP-54	always	accept	Enabled
85	vdom_link11	vlan_112A°	192.168.50.11/32	N/A	192.168.112.11/32	tcp_443 tcp_80	N/A	OP-55	always	accept	Enabled
90	any	any	20.20.20.20/32	N/A	30.30.30.30/32	tcp_80	N/A	OP-64	always	accept	Enabled
93	any	any	7.7.7.7/32	N/A	8.8.8/32 9.9.9.9/32	tcp_78 tcp_87	N/A	OP-167	2023_07_20T00:00	accept	Enabled
94	any	any	8.8.8/32	N/A	7.7.7/32 9.9.9.9/32	tcp_78 tcp_87	N/A	OP-167OP-170	2023_07_20T00:00	accept	Enabled
98	any	any	13.15.16.16/32	N/A	8.8.8/32 test.com	tcp_445	N/A	OP-5982	always	accept	Enabled

 Palo_Alto_1 # Rules on Risky Services or Protocols: 186 | Total Rules: 386

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
ipsec	any	any	10.34.128.201 10.34.128.203	N/A	10.34.128.201 10.34.128.203	any	any		always	accept	Enabled
Jupiter Int Erisimi	test_ui	untrust	JUPITER01-172.22.3.177 JUPITER02-172.22.3.178	N/A	134.170.94.0/24 185.152.252.0/22 204.79.197.0/24 216.58.209.0/24 maps-172.217.16.0 maps-172.217.18.0 maps-172.217.20.0 maps.googleapis.com	service-http service-https	any	OP-431	always	accept	Disabled
usom2	test_db	test_ui untrust	fortiguard usom	N/A	192.168.132.150_32 192.168.133.10-192.168.133.50	tcp_10	any	OP-1	always	accept	Enabled
OP-1-2	test_db	test_ui untrust	usom 192.147.15.26_32	N/A	192.168.30.30_31 192.168.40.4-192.168.40.20 192.168.50.5_32 192.147.15.26_32	tcp_10	any	OP-1-dstcck3-OP-5666	always	accept	Enabled
OP-1	test_db	test_ui untrust	192.168.140.50_32	N/A	192.168.133.10-192.168.133.50 192.168.132.150_32	tcp_10	any	OP-1	always	accept	Enabled
usom2-1	test_db	test_ui untrust	AZ CU	N/A	192.168.132.150_32 192.168.133.10-192.168.133.50	tcp_10	any	anil2anil3-OP-137	always	accept	Enabled
OP-295-3-i	untrust	test_db test_ui	192.168.50.73_32	N/A	192.168.133.121_32 192.168.140.53_32	any	icmp	OP-295-3-OP-57-OP-5276	always	accept	Enabled
OP-295-5	untrust	test_db	192.168.50.73_32	N/A	192.168.140.73_32	tcp_443 tcp_445	any	OP-295-5	always	accept	Enabled
OP-295-6	test_db	untrust	192.168.140.73_32	N/A	192.168.50.73_32	tcp_443 tcp_445	any	OP-295-6	always	accept	Enabled
OP-295-7-i	untrust	test_ui	192.168.50.73_32	N/A	192.168.133.126_32	any	icmp	OP-295-7	always	accept	Enabled
OP-363	untrust	test_db	192.168.83.26_32 192.168.73.26_32	N/A	192.168.140.26_32	tcp_445 udp_445	any	OP-363-OP-372	2023_08_09T00_00	accept	Enabled
OP-383	untrust	test_db	192.168.83.27_32 10.0.0.27_32	N/A	192.168.140.27_32	tcp_80 tcp_23	any	OP-383	2023_08_09T00_00	accept	Enabled
OP-384	untrust	test_db	192.168.50.27_32	N/A	192.168.140.27_32	tcp_80 tcp_23	any	OP-384	2023_08_09T00_00	accept	Enabled
OP-390	untrust	test_db	192.168.83.25_32 192.168.73.25_32 10.0.0.25_32	N/A	192.168.140.25_32	tcp_445 tcp_443	any	OP-390-OP-410	2023_08_09T00_00	accept	Enabled
OP-395	untrust	test_db	192.168.83.30_32 10.0.0.30_32	N/A	192.168.140.30_32	tcp_443 tcp_80	any	OP-395	always	accept	Enabled
OP-411	untrust	test_db	192.168.83.25_32	N/A	192.168.140.25_32	tcp_443 tcp_80	any	OP-411	always	accept	Enabled
OP-437	untrust	test_db	192.168.83.20_32 192.168.50.20_32	N/A	192.168.140.20_32	tcp_443 tcp_445	any	OP-437-OP-466	always	accept	Enabled
OP-447	untrust	test_db	192.168.83.20_32 4.4.4.4_32	N/A	192.168.140.20_32	tcp_80	any	test	always	accept	Enabled
OP-4970	linux_zone	untrust	192.168.170.10_32	N/A	192.168.40.10_32	tcp_80	any	OP-4970	always	accept	Enabled
OP-455-1	untrust	test_db	192.168.50.26_32	N/A	192.168.140.26_32	tcp_445 udp_445	any	OP-455-1	2023_08_09T00_00	accept	Enabled

 FG_Opinrate_2 | root # Rules on Risky Services or Protocols: 40 | Total Rules: 167

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
126	any	any	8.8.8/32	N/A	7.7.7.7/32	tcp_78 tcp_87	N/A	OP-167	2023_07_20T00:00	accept	Enabled
18	port1 cp_net port2	cp_net port1	10.0.0.110 10.0.0.111 178.157.15.222/32	N/A	10.0.0.110 10.0.0.111 178.157.15.222/32	any	N/A	OP-59	always	accept	Enabled
125	cp_net port2	port1 cp_net port2	10.0.0.110 10.0.0.111 10.0.0.112	N/A	any	any	N/A	Reverseof1	always	accept	Enabled
1	port1 cp_net port2	cp_net port2	any	N/A	10.0.0.110 10.0.0.111 10.0.0.112	any	N/A		always	accept	Enabled
22	any	any	Mobile-app	N/A	Database-grp	tcp_443 tcp_80	N/A	OP-61	always	accept	Enabled
29	port1	cp_net	192.168.51.0/24 192.168.52.0/24	N/A	192.168.73.73/32	tcp_80	N/A	OP-84	always	accept	Enabled
31	cp_net	port1 vdom_link10	192.168.73.73/32	N/A	3.3.3.3/32 1.3.3.3/32 192.168.50.50/32 192.168.30.30/32 192.168.93.0/24 192.168.112.0/24 192.168.5.5/32	any	N/A	OP-84	always	accept	Enabled
58	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
63	any	any	A_grp_1	N/A	B_grp_2	udp_11	N/A	OP-868	always	accept	Enabled
64	any	any	A_grp_1	N/A	B_grp_2	tcp_11	N/A	OP-887	always	accept	Enabled
65	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
66	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
69	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
70	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
71	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
72	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
73	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
74	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
75	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
76	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled

 PaloAlto_2 # Rules on Risky Services or Protocols: 41 | Total Rules: 66

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
OP-1	external	prod_db	192.168.140.50_32 192.168.30.30_32	N/A	192.168.132.150_32	tcp_10	any	anil2-OP-5000	always	accept	Enabled

usom-1	any	any	fortiguard usom	N/A	2.2.2.2_32 8.8.8.8_32	tcp_12 tcp_21 tcp_89 tcp_98 udp_89 udp_98	any	Opinnate131testOP-483	2023_07_22T00_00	accept	Enabled
usom	any	any	usom	N/A	2.2.2.2_32	tcp_12 tcp_21 tcp_89 tcp_98 udp_89 udp_98	any	Opinnate131testanil3OP-46-0...	always	accept	Enabled
OP-17-1	any	any	9.9.9.9_32	N/A	2.2.2.2_32	tcp_89 tcp_98 udp_89 udp_98 tcp_12 tcp_21	any	a1b2anil3-CANCAN-OP-254	2023_07_22T00_00	accept	Enabled
OP-295	prod_app	external	192.168.52.0_24 192.168.30.69_32	N/A	192.168.50.73_32	tcp_80	any	OP-295-OP-5005	always	accept	Enabled
OP-295-3-i	external	prod_db	192.168.50.73_32	N/A	192.168.132.188_32 192.168.132.181_32	any	icmp	revreplaceComment	always	accept	Enabled
OP-295-5-i	external	prod_db	192.168.50.73_32	N/A	192.168.132.169_32	any	icmp	aas	always	accept	Enabled
OP-659	any	any	5.5.5.5_32	N/A	6.6.6.6_32	tcp_80 tcp_81	any	OP-659	2023_09_10T00_00	accept	Disabled
commen-Policy-i	external	prod_db	192.168.170.15_32 192.168.170.16_32 192.168.170.24_32	N/A	192.168.180.17_32	any	icmp	commen-Policy-OP-32	always	accept	Enabled
OP-43	external	prod_db	192.168.12.44_32	N/A	192.168.132.174_32	tcp_80 tcp_443 tcp_3125-5588	any	OP-43	always	accept	Enabled
OP-51	prod_db prod_app	external	any	N/A	192.168.150.17_32 192.168.170.55_32 192.168.133.14_32	tcp_99-195 tcp_66 udp_73	any	OP-51	always	accept	Enabled
OP-51-i	prod_db prod_app	external	192.168.140.50_32 2.2.2.2_32	N/A	192.168.150.17_32 192.168.170.55_32 192.168.133.14_32	any	icmp	OP-51-	always	accept	Enabled
OP-56	prod_db prod_app	external	any 192.168.170.15_32 192.168.140.15_32	N/A	192.168.133.26_32 192.168.112.25_32	tcp_99-195 tcp_66 udp_73	any	OP-56-cck1	always	accept	Enabled
OP-56-i	prod_db prod_app	external	any 192.168.170.15_32 192.168.140.15_32 192.168.40.41_32 192.168.83.83-192.168.83.90	N/A	192.168.133.26_32 192.168.112.25_32	any	icmp	OP-56-cck1--cck2	always	accept	Enabled
OI-22-i	any	any	192.168.23.26_32	N/A	192.168.25.36_32	any	icmp	OI-22	always	accept	Disabled
OP-5230	any	any	192.168.36.29_32	N/A	168.27.15.48_32	tcp_23	any	OP-5230	always	accept	Enabled
OP-5230-i	any	any	192.168.36.29_32	N/A	168.27.15.48_32	any	icmp	OP-5230	always	accept	Enabled
OP-5273	any	any	192.168.73.10_32	N/A	192.168.132.128_25	any	any	OP-5273Test-1	always	accept	Enabled
OP-5273-1	any	any	192.168.132.128_25 192.168.40.41_32 192.168.83.83-192.168.83.90	N/A	192.168.73.10_32 172.16.2.0_24	any	any	OP-5273Test-1--cck2-vs-cck4...	always	accept	Enabled
OP-5420-i	any	any	44.41.2.4_32 192.168.25.36_32 172.35.68.69_32 192.168.16.17_32 192.168.17.18_32	N/A	12.3.31.4_32 192.168.25.36_32 172.35.68.69_32 172.16.2.0_24 192.168.20.23_32 192.168.132.130_32 192.168.16.17_32 192.168.17.18_32	any	icmp	ali-replace-vs-cck4-OP-5730...	always	accept	Enabled

cp-2sms | vs_3rd_party

No Data

cp-sms2 | vs_opinnate

No Data

cp-sms1 | cp-node # Rules on Risky Services or Protocols: 1 | Total Rules: 9

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
8	any	any	any	N/A	cp-node	ssh_version_2 ssh echo-reply echo-request https	any		always	accept	Enabled

PA3000-OP3 # Rules on Risky Services or Protocols: 12 | Total Rules: 28

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
cp-sms-spark	cp_spark_zone fg1_zone	cp_spark_zone fg1_zone	10.0.0.110 cp-192.168.160.1	N/A	10.0.0.110 cp-192.168.160.1	any	any		always	accept	Enabled
cp-spark-erisim	untrust	any	op-net-10.34.128.0_23	N/A	any	any	any	OP-288OP-289	always	accept	Enabled
OP-372	untrust	cp_spark_zone	192.168.50.15_32 192.168.40.15_32	N/A	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	udp_445 udp_88 udp_389 tcp_53 tcp_445	any	OP-372	2023_09_27T00_00	accept	Enabled
OP-372-i	untrust	cp_spark_zone	192.168.50.15_32 192.168.40.15_32	N/A	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	any	icmp	OP-372	2023_09_27T00_00	accept	Enabled
OP-372-1	cp_spark_zone	untrust	192.168.83.30_32 192.168.69.71_32	N/A	192.168.50.15_32 192.168.40.15_32 192.168.180.17_32	udp_445 udp_88 udp_389 tcp_53 tcp_445	any	OP-372--OP-5752	2023_09_27T00_00	accept	Enabled
OP-372-1-i	cp_spark_zone	untrust	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	N/A	192.168.50.15_32 192.168.40.15_32	any	icmp	OP-372	2023_09_27T00_00	accept	Enabled
OP-379	untrust	cp_spark_zone	192.168.120.55_32 192.168.120.56_32 1.1.1.1_32	N/A	192.168.160.3_32 192.168.160.4_32 1.1.1.1_32	tcp_444 tcp_445 udp_445	any	OP-379-OP-490-OP-491-OP-492...	always	accept	Enabled
OP-458	untrust cp_spark_zone	untrust	any	N/A	172.145.21.3_32 172.35.68.69_32	tcp_445	any	test	always	accept	Enabled
OP-458-1	untrust cp_spark_zone	untrust fg1_zone	any	N/A	172.168.36.23_32 192.168.133.9-192.168.133.49 172.35.68.69_32	tcp_66 tcp_42 tcp_21 tcp_43	any	testupdate	always	accept	Enabled
OP-610	any	any	192.168.59.63_32	N/A	172.14.15.23_32	tcp_21 tcp_34 tcp_41 tcp_56	any	OP-610	always	accept	Enabled
OP-5741	any	any	172.145.47.88_32	N/A	162.251.78.0_24	tcp_21 tcp_41 tcp_55 tcp_66	any	OP-5741OP-5897	always	accept	Disabled
OP-5976	any	any	192.168.133.10_32	N/A	192.168.83.86_32	tcp_3389	any	OP-5976	2023_11_09T00_00	accept	Enabled

No Data

Usage of The Rules on Firewalls

Rules that are not used must be removed from the firewalls. Here is the list of first 20 rules on each firewall that are not used.

Unused Rules	2
Total Rules	1217



cp_cluster | cp-cluster # Unused Rules: 1 | Total Rules: 12

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
11	any	any	any	N/A	cp-gateway1 cp-cluster	any	any		always	accept	Enabled



FG_Opinnate_1

No Data



FG_Opinnate_2 | Customer_vd

No Data



Palo_Alto_1

No Data



FG_Opinnate_2 | root

No Data



PaloAlto_2

No Data



cp-2sms | vs_3rd_party

No Data



cp-sms2 | vs_opinnate

No Data



cp-sms1 | cp-node # Unused Rules: 1 | Total Rules: 9

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
8	any	any	any	N/A	cp-node	ssh_version_2 ssh echo-reply echo-request https	any		always	accept	Enabled



PA3000-OP3

No Data




PA-Opinnate-v9


No Data

Shadow Status of Rules

Rules shadowed by any other rule must be removed since they are non-functional. Here is the list of first 20 rules on each firewall that are shadowed.

Shadowed Rules	132
Total Rules	1217

 cp_cluster | cp-cluster
No Data

 FG_Opinstate_1 # Shadowed Rules: 35 | Total Rules: 453

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	649	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled
Shadowed	639	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	649	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled
Shadowed	640	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	649	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled
Shadowed	641	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	649	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled
Shadowed	646	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	649	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled
Shadowed	647	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	598	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32 10.0.0.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 10.0.0.10/32	tcp_21	N/A	OP-5936	always	accept	Enabled
Shadowed	683	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5883OP-5904	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	598	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32 10.0.0.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 10.0.0.10/32	tcp_21	N/A	OP-5936	always	accept	Enabled
Shadowed	684	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5883OP-5904	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	598	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32 10.0.0.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 10.0.0.10/32	tcp_21	N/A	OP-5936	always	accept	Enabled
Shadowed	685	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5883OP-5904	always	accept	Enabled


	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	598	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32 10.0.0.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 10.0.0.10/32	tcp_21	N/A	OP-5936	always	accept	Enabled
Shadowed	686	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5883OP-5904	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status

Master	598	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32 10.0.0.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 10.0.0.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5936	always	accept	Enabled
Shadowed	698	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 10.0.0.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5903	always	accept	Enabled

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status	
Master	598	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32 10.0.0.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 10.0.0.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5936	always	accept	Enabled
Shadowed	699	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 10.0.0.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5903	always	accept	Enabled

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status	
Master	598	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32 10.0.0.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 10.0.0.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5936	always	accept	Enabled
Shadowed	700	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 10.0.0.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5903	always	accept	Enabled

 FG_Opinrate_2 | Customer_vd # Shadowed Rules: 12 | Total Rules: 96

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	7	port6	vlan_112A°	any	any	any	N/A		always	deny	Enabled
Shadowed	2	port6	vlan_112A°	50.50.50.50/32	N/A	autoupdate.opera.com	HTTP HTTPS	N/A	always	accept	Enabled

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status	
Master	3	any	any	50.50.50.50/32	N/A	49.50.50.50/32	udp_44	N/A	OP-243	always	accept	Enabled
Shadowed	1	any	any	50.50.50.50/32	N/A	49.50.50.50/32	udp_44	N/A	OP-243	always	accept	Enabled

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status	
Master	33	vdom_link11	vlan_112A°	192.168.73.73/32	N/A	192.168.112.0/24	any	N/A	OP-84	always	accept	Enabled
Shadowed	32	vdom_link11	vlan_112A°	192.168.73.73/32	N/A	192.168.112.168/32 192.168.112.50/32 192.168.112.36/32 192.168.112.85/32 192.168.112.92/32 192.168.112.53/32	ALL_ICMP	N/A	OP-84	always	accept	Enabled

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status	
Master	56	any	any	A_grp_1	N/A	B_grp_2	tcp_443	N/A	OP-4286	always	accept	Enabled
Shadowed	75	any	any	A_grp_1	N/A	B_grp_2	tcp_443	N/A	OP-4349	always	accept	Enabled

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status	
Master	56	any	any	A_grp_1	N/A	B_grp_2	tcp_443	N/A	OP-4286	always	accept	Enabled
Shadowed	74	any	any	A_grp_1	N/A	B_grp_2	tcp_443	N/A	OP-4348	always	accept	Enabled

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status	
Master	62	vlan_112A°	vdom_link11	192.168.112.50/32 192.168.112.36/32 192.168.112.85/32 192.168.112.92/32 192.168.112.53/32 192.168.112.126/32	N/A	192.168.99.50/32	any	N/A	OP-4342	always	accept	Enabled
Shadowed	67	vlan_112A°	vdom_link11	192.168.112.50/32	N/A	192.168.99.50/32	tcp_443 ALL_ICMP	N/A	OP-4342	always	accept	Enabled

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status	
Master	61	vdom_link11	vlan_112A°	192.168.99.50/32	N/A	192.168.112.58/32 192.168.112.112/32	any	N/A	OP-4342	always	accept	Enabled
Shadowed	63	vdom_link11	vlan_112A°	192.168.99.50/32	N/A	192.168.112.112/32	udp_42323 tcp_443 ALL_ICMP udp_80	N/A	OP-4342	always	accept	Enabled

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status	
Master	57	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled
Shadowed	59	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status	
Master	52	any	any	15.15.15.36/32	N/A	19.15.16.16/32	ALL_ICMP	N/A	OP-4269	always	accept	Enabled
Shadowed	55	any	any	15.15.15.36/32	N/A	19.15.16.16/32	ALL_ICMP	N/A	OP-4269	always	accept	Enabled

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status	
Master	52	any	any	15.15.15.36/32	N/A	19.15.16.16/32	ALL_ICMP	N/A	OP-4269	always	accept	Enabled
Shadowed	54	any	any	15.15.15.36/32	N/A	19.15.16.16/32	ALL_ICMP	N/A	OP-4269	always	accept	Enabled

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status	
Master	52	any	any	15.15.15.36/32	N/A	19.15.16.16/32	ALL_ICMP	N/A	OP-4269	always	accept	Enabled
Shadowed	53	any	any	15.15.15.36/32	N/A	19.15.16.16/32	ALL_ICMP	N/A	OP-4269	always	accept	Enabled

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status	
Master	96	any	any	32.44.55.66/32	N/A	192.168.16.35/32	tcp_1326	N/A	OP-5296	always	accept	Enabled
Shadowed	95	any	any	32.44.55.66/32	N/A	192.168.16.35/32	tcp_1326	N/A	OP-Ali	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	caaaaaaaaaaaaaaaaa-3	test_db untrust	test_app	192.168.140.20_32 192.168.50.20_32 8.8.8.8_32 10.0.0.20_32 7.7.7.7_32 10.0.0.10_32 10.0.0.11_32 18.19.12.12_32	N/A	192.168.150.17_32	tcp_443 udp_4456 udp_445	any	caaaaaaaaaaaaaaaaa-3-OP-62-O...	always	accept	Enabled
Shadowed	OP-5216-3	test_db untrust	test_app	192.168.140.20_32 192.168.50.20_32 8.8.8.8_32 10.0.0.20_32 7.7.7.7_32 10.0.0.10_32	N/A	192.168.150.17_32	tcp_443 udp_4456 udp_445	any	OP-5216-3-OP-62-OP-53...	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	caaaaaaaaaaaaaaaaa-10	test_db untrust	test_app	192.168.140.20_32 1.1.1.8_32 192.168.1.61_32	N/A	192.168.150.17_32	tcp_444 tcp_81 tcp_82 tcp_443 udp_4456	any	caaaaaaaaaaaaaaaaa-10	always	accept	Enabled
Shadowed	OP-5216-9	test_db	test_app	192.168.140.20_32	N/A	192.168.150.17_32	tcp_443 udp_4456	any	OP-5216-9	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	caaaaaaaaaaaaaaaaa-10	test_db untrust	test_app	192.168.140.20_32 1.1.1.8_32 192.168.1.61_32	N/A	192.168.150.17_32	tcp_444 tcp_81 tcp_82 tcp_443 udp_4456	any	caaaaaaaaaaaaaaaaa-10	always	accept	Enabled
Shadowed	OP-5216-10	test_db untrust	test_app	192.168.140.20_32 1.1.1.8_32 192.168.1.61_32	N/A	192.168.150.17_32	tcp_444 tcp_81 tcp_82 tcp_443 udp_4456	any	OP-5216-10	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	caaaaaaaaaaaaaaaaa-2	untrust test_db	test_app	10.0.0.20_32 5.5.5.5_32 192.168.140.20_32 8.8.8.8_32 55.55.55.55_32	N/A	192.168.150.17_32	tcp_443 tcp_445 tcp_444	any	caaaaaaaaaaaaaaaaa-2-OP-631	always	accept	Enabled
Shadowed	izmir-2	untrust test_db	test_app	10.0.0.20_32 5.5.5.5_32 192.168.140.20_32 8.8.8.8_32 55.55.55.55_32	N/A	192.168.150.17_32	tcp_443 tcp_445 tcp_444	any	izmir-2-OP-631	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	caaaaaaaaaaaaaaaaa-3	test_db untrust	test_app	192.168.140.20_32 192.168.50.20_32 8.8.8.8_32 10.0.0.20_32 7.7.7.7_32 10.0.0.10_32 10.0.0.11_32 18.19.12.12_32	N/A	192.168.150.17_32	tcp_443 udp_4456 udp_445	any	caaaaaaaaaaaaaaaaa-3-OP-62-O...	always	accept	Enabled
Shadowed	izmir-3	test_db untrust	test_app	192.168.140.20_32 192.168.50.20_32 8.8.8.8_32 10.0.0.20_32 7.7.7.7_32 10.0.0.10_32 10.0.0.11_32	N/A	192.168.150.17_32	tcp_443 udp_4456 udp_445	any	izmir-3-OP-634	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	caaaaaaaaaaaaaaaaa-5	test_app	untrust test_db	192.168.150.17_32	N/A	192.168.50.20_32 10.0.0.20_32 192.168.140.20_32 10.0.0.10_32	tcp_81 tcp_82	any	caaaaaaaaaaaaaaaaa-5	always	accept	Enabled
Shadowed	izmir-5	test_app	untrust test_db	192.168.150.17_32	N/A	192.168.50.20_32 10.0.0.20_32 192.168.140.20_32 10.0.0.10_32	tcp_81 tcp_82	any	izmir-5	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	caaaaaaaaaaaaaaaaa-3	test_db untrust	test_app	192.168.140.20_32 192.168.50.20_32 8.8.8.8_32 10.0.0.20_32 7.7.7.7_32 10.0.0.10_32 10.0.0.11_32 18.19.12.12_32	N/A	192.168.150.17_32	tcp_443 udp_4456 udp_445	any	caaaaaaaaaaaaaaaaa-3-OP-62-O...	always	accept	Enabled
Shadowed	caaaaaaaaaaaaaaaaa	untrust	test_app	192.168.50.20_32	N/A	192.168.150.17_32	tcp_443	any	caaaaaaaaaaaaaaaaa	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	caaaaaaaaaaaaaaaaa-10	test_db untrust	test_app	192.168.140.20_32 1.1.1.8_32 192.168.1.61_32	N/A	192.168.150.17_32	tcp_444 tcp_81 tcp_82 tcp_443 udp_4456	any	caaaaaaaaaaaaaaaaa-10	always	accept	Enabled
Shadowed	caaaaaaaaaaaaaaaaa-9	test_db	test_app	192.168.140.20_32	N/A	192.168.150.17_32	tcp_443 udp_4456	any	caaaaaaaaaaaaaaaaa-9	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	OP-5230-1	any	any	192.168.36.29_32	N/A	168.27.15.48_32	tcp_23	any	OP-5230-1	always	accept	Enabled
Shadowed	OP-5230	any	any	192.168.36.29_32	N/A	168.27.15.48_32	tcp_23	any	OP-5230	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	OP-5230-1-i	any	any	192.168.36.29_32	N/A	168.27.15.48_32	any	icmp	OP-5230-1	always	accept	Enabled
Shadowed	OP-5230-i	any	any	192.168.36.29_32	N/A	168.27.15.48_32	any	icmp	OP-5230	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	OP-627	untrust	test_db	192.168.40.10_32	N/A	192.168.140.10_32	tcp_445 tcp_43 tcp_44 tcp_447 tcp_333 tcp_444 tcp_446 tcp_448 tcp_449 tcp_443 tcp_459	any	OP-627	always	accept	Enabled
Shadowed	OP-317	untrust	test_db	192.168.40.10_32	N/A	192.168.140.10_32	tcp_447 tcp_443	any	OP-317	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status

Master	OP-627	untrust	test_db	192.168.40.10_32	N/A	192.168.140.10_32	tcp_445 tcp_43 tcp_44 tcp_447 tcp_333 tcp_444 tcp_446 tcp_448 tcp_449 tcp_443 tcp_459	any	OP-627	always	accept	Enabled
Shadowed	OP-592	untrust	test_db	192.168.40.10_32	N/A	192.168.140.10_32	tcp_445 tcp_43 tcp_44 tcp_447 tcp_333 tcp_444 tcp_446 tcp_448 tcp_443 tcp_459	any	OP-592	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	OP-627-2	linux_zone test_db	untrust	192.168.170.48_32 192.168.140.53_32 192.168.170.36_32 192.168.170.26_32	N/A	192.168.40.10_32	udp_44	any	OP-627-2	always	accept	Enabled
Shadowed	OP-592-1	linux_zone test_db	untrust	192.168.170.48_32 192.168.140.53_32 192.168.170.36_32 192.168.170.26_32	N/A	192.168.40.10_32	udp_44	any	OP-592-1	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	OP-627-5	untrust	test_db	192.168.40.10_32	N/A	192.168.140.155_32	tcp_61	any	OP-627-5	always	accept	Enabled
Shadowed	OP-592-2	untrust	test_db	192.168.40.10_32	N/A	192.168.140.155_32	tcp_61	any	OP-592-2	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	OP-627-7	untrust	test_db asa_zone	192.168.40.10_32	N/A	192.168.140.10_32 172.16.2.0_24 192.168.140.0_24	tcp_443	any	OP-627-7	always	accept	Enabled
Shadowed	OP-592-3	untrust	test_db asa_zone	192.168.40.10_32	N/A	192.168.140.10_32 172.16.2.0_24	tcp_443	any	OP-592-3	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	OP-627-8	untrust	asa_zone test_ui test_db test_app test_app2	192.168.40.10_32	N/A	any	tcp_444	any	OP-627-8	always	accept	Enabled
Shadowed	OP-592-4	untrust	asa_zone test_ui test_db test_app test_app2	192.168.40.10_32	N/A	any	tcp_444	any	OP-592-4	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	OP-653-5	untrust linux_zone	linux_zone untrust	192.168.112.92_32 192.168.112.126_32 192.168.112.53_32 192.168.30.29_32 11.1.1.1_32 192.168.170.53_32 192.168.80.52_32 178.157.15.29_32	N/A	192.168.170.53_32 192.168.50.10_32 192.168.40.10_32 192.168.112.92_32 192.168.112.126_32 192.168.112.53_32 192.168.30.29_32 192.168.80.52_32 11.1.1.1_32 192.168.50.11_32 192.168.120.10_32 192.168.50.11_32 178.157.15.29_32 11.1.1.1	tcp_21	any	OP-653-5-OP-674-OP-5904-OP-...	always	accept	Enabled
Shadowed	OP-592-5	untrust linux_zone	linux_zone untrust	192.168.112.92_32 192.168.112.126_32 192.168.112.53_32 192.168.30.29_32 11.1.1.1_32 192.168.170.53_32 192.168.80.52_32 178.157.15.29_32	N/A	192.168.170.53_32 192.168.112.92_32 192.168.112.126_32 192.168.112.53_32 192.168.30.29_32 11.1.1.1_32 192.168.80.52_32 192.168.40.10_32 192.168.50.11_32 178.157.15.29_32 11.1.1.1	tcp_21	any	OP-592-5-OP-616-OP-629-OP-6...	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	OP-5883-11	untrust	test_db	192.168.0.0/16 192.168.120.10_32	N/A	192.168.140.53_32	udp_44	any	OP-5883-11	always	accept	Enabled
Shadowed	OP-592-6	untrust	test_db	192.168.40.10_32	N/A	192.168.140.53_32	udp_44	any	OP-592-6	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	OP-653-7	untrust	test_db asa_zone	192.168.120.10_32	N/A	192.168.140.10_32 172.16.2.0_24 192.168.140.0_24	tcp_443	any	OP-653-7	always	accept	Enabled
Shadowed	OP-608	untrust	test_db	192.168.120.10_32	N/A	192.168.140.12_32 192.168.140.10_32	tcp_443	any	OP-608	always	accept	Enabled

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	OP-653-5	untrust linux_zone	linux_zone untrust	192.168.112.92_32 192.168.112.126_32 192.168.112.53_32 192.168.30.29_32 11.1.1.1_32 192.168.170.53_32 192.168.80.52_32 178.157.15.29_32	N/A	192.168.170.53_32 192.168.50.10_32 192.168.40.10_32 192.168.112.92_32 192.168.112.126_32 192.168.112.53_32 192.168.30.29_32 192.168.80.52_32 11.1.1.1_32 192.168.50.11_32 192.168.120.10_32 192.168.50.11_32 178.157.15.29_32 11.1.1.1	tcp_21	any	OP-653-5-OP-674-OP-5904-OP-...	always	accept	Enabled
Shadowed	OP-627-3	untrust linux_zone	linux_zone untrust	192.168.112.92_32 192.168.112.126_32 192.168.112.53_32 192.168.30.29_32 11.1.1.1_32 192.168.170.53_32 192.168.80.52_32	N/A	192.168.170.53_32 192.168.50.10_32 192.168.40.10_32 192.168.112.92_32 192.168.112.126_32 192.168.112.53_32 192.168.30.29_32 192.168.80.52_32 11.1.1.1_32 192.168.50.11_32 192.168.50.11_32 178.157.15.29_32	tcp_21	any	OP-627-3-OP-639-OP-674-OP-5...	always	accept	Enabled


 FG Opinnate_2 | root # Shadowed Rules: 29 | Total Rules: 167

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	171	any	any	192.120.13.8/32 192.168.16.30/32 192.168.20.0/24 192.168.16.32/32	N/A	192.138.12.71/32 192.148.13.70/32 192.128.9.71-192.128.11.40	tcp_10010 tcp_10011 ALL_ICMP udp_10010	N/A	fmg-ali-1aa	always	accept	Enabled


Shadowed	167	any	any	192.120.13.8/32	N/A	192.138.12.71/32 192.148.13.70/32 192.128.9.71-192.128.11.40	tcp_10010 tcp_10011 ALL_ICMP udp_10010	N/A	fmg-ali-1	2023_11_21T22:41	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	96	any	any	A_grp_1	N/A	B_grp_2	tcp_443	N/A	OP-4349	always	accept	Enabled
Shadowed	57	any	any	A_grp_1	N/A	B_grp_2	tcp_443	N/A	OP-4286	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	76	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
Shadowed	58	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	96	any	any	A_grp_1	N/A	B_grp_2	tcp_443	N/A	OP-4349	always	accept	Enabled
Shadowed	59	any	any	A_grp_1	N/A	B_grp_2	tcp_443	N/A	OP-815	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	96	any	any	A_grp_1	N/A	B_grp_2	tcp_443	N/A	OP-4349	always	accept	Enabled
Shadowed	60	any	any	A_grp_1	N/A	B_grp_2	tcp_443	N/A	OP-813	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	76	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
Shadowed	65	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	76	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
Shadowed	66	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	79	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled
Shadowed	67	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	79	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled
Shadowed	68	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	76	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
Shadowed	69	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	76	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
Shadowed	70	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	76	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
Shadowed	71	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	76	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
Shadowed	72	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	76	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
Shadowed	73	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	76	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
Shadowed	74	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	76	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
Shadowed	75	any	any	A_grp_1	N/A	B_grp_2	tcp_22	N/A	234324234234	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	79	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled
Shadowed	78	any	any	A_grp_1	N/A	A_grp_1	tcp_11111	N/A	OP-1749	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	89	vdom_link10 port1	port1 vdom_link10	192.168.112.50/32 1.3.3.3/32 192.168.99.50/32	N/A	192.168.50.50/32 192.168.30.30/32 1.3.3.3/32 192.168.99.50/32 192.168.112.50/32	any	N/A	OP-4342	always	accept	Enabled
Shadowed	86	vdom_link10 port1	port1 vdom_link10	192.168.112.50/32 192.168.99.50/32	N/A	192.168.30.30/32 192.168.99.50/32 192.168.112.50/32	ALL_ICMP	N/A	OP-4342	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	89	vdom_link10 port1	port1 vdom_link10	192.168.112.50/32 1.3.3.3/32 192.168.99.50/32	N/A	192.168.50.50/32 192.168.30.30/32 1.3.3.3/32 192.168.99.50/32 192.168.112.50/32	any	N/A	OP-4342	always	accept	Enabled
Shadowed	87	vdom_link10	port1	192.168.112.50/32	N/A	192.168.99.50/32	tcp_443 ALL_ICMP	N/A	OP-4342	always	accept	Enabled
	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	89	vdom_link10 port1	port1 vdom_link10	192.168.112.50/32 1.3.3.3/32 192.168.99.50/32	N/A	192.168.50.50/32 192.168.30.30/32 1.3.3.3/32 192.168.99.50/32 192.168.112.50/32	any	N/A	OP-4342	always	accept	Enabled
Shadowed	88	vdom_link10 port1	port1 vdom_link10	192.168.112.50/32 192.168.99.50/32	N/A	192.168.50.50/32 192.168.30.30/32 192.168.99.50/32 192.168.112.50/32	any	N/A	OP-4342	always	accept	Enabled

 PaloAlto_2

No Data

 cp-2sms | vs_3rd_party

No Data

 cp-sms2 | vs_opinnate

No Data



cp-sms1 | cp-node # Shadowed Rules: 5 | Total Rules: 9

	Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
Master	2	any	any	1.2.1.2	N/A	2.1.2.1 2.1.1.1	tcp_3390	any	OP-789OP-6973OP-6974OP-5994	always	accept	Enabled
Shadowed	7	any	any	1.2.1.2	N/A	2.1.2.1	tcp_3390	any	OP-789	always	accept	Enabled
Master	2	any	any	1.2.1.2	N/A	2.1.2.1 2.1.1.1	tcp_3390	any	OP-789OP-6973OP-6974OP-5994	always	accept	Enabled
Shadowed	6	any	any	1.2.1.2	N/A	2.1.2.1	tcp_3390	any	OP-789	always	accept	Enabled
Master	2	any	any	1.2.1.2	N/A	2.1.2.1 2.1.1.1	tcp_3390	any	OP-789OP-6973OP-6974OP-5994	always	accept	Enabled
Shadowed	5	any	any	1.2.1.2	N/A	2.1.2.1	tcp_3390	any	OP-789	always	accept	Enabled
Master	2	any	any	1.2.1.2	N/A	2.1.2.1 2.1.1.1	tcp_3390	any	OP-789OP-6973OP-6974OP-5994	always	accept	Enabled
Shadowed	4	any	any	1.2.1.2	N/A	2.1.2.1	tcp_3390	any	OP-789xprojesi	always	accept	Enabled
Master	2	any	any	1.2.1.2	N/A	2.1.2.1 2.1.1.1	tcp_3390	any	OP-789OP-6973OP-6974OP-5994	always	accept	Enabled
Shadowed	3	any	any	1.2.1.2	N/A	2.1.2.1	tcp_3390	any	OP-789xprojesi	always	accept	Enabled



PA3000-OP3

No Data



PA-Opinnate-v9

No Data

Expiry Status of The Rules

Rules that are expired have no function so they must be removed. Here is the list of first 20 rules on each firewall that are expired.

Expired Rules	77
Total Rules	1217

 cp_cluster | cp-cluster # Expired Rules: 2 | Total Rules: 12

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
10	any	any	192.168.133.10	N/A	192.168.83.86	Tcp_3389	any	OP-5976	091123T0000	accept	Enabled
2	any	any	10.0.0.100	N/A	10.115.207.100	Tcp_3389 tcp_3389	any	OP-5995	101123T0000	accept	Enabled

 FG_Opinntate_1 # Expired Rules: 2 | Total Rules: 453

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
579	any	any	5.5.5.32	N/A	6.6.6.6/32 4.4.4.4/32	tcp_80 tcp_81	N/A	OP-659OP-65	2023_09_10T00:00	accept	Enabled
624	port3	sd-wan3	192.168.50.10/32	N/A	192.168.140.155/32	udp_445	N/A	OP-68	2023_09_22T00:00	accept	Enabled

 FG_Opinntate_2 | Customer_vd # Expired Rules: 12 | Total Rules: 96

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
48	vdom_link11	vlan_112A*	192.168.83.222/32 192.168.140.222/32	N/A	192.168.112.222/32	tcp_443 tcp_80	N/A	OP-113	2023_06_30T00:00	accept	Enabled
49	vdom_link11	vlan_112A*	192.168.30.222/32	N/A	192.168.112.222/32	tcp_443 tcp_80	N/A	differentcomment	2023_06_30T00:00	accept	Enabled
50	vdom_link11	vlan_112A*	192.168.140.12/32	N/A	192.168.112.12/32	tcp_443	N/A	test	2023_07_26T00:00	accept	Enabled
51	vlan_112A*	vdom_link11	192.168.112.12/32	N/A	192.168.140.12/32	tcp_443	N/A	test	2023_07_26T00:00	accept	Enabled
60	vdom_link11	vlan_112A*	192.168.140.12/32	N/A	192.168.112.12/32	tcp_444	N/A	OP-26OP-27OP-28	2023_07_20T00:00	accept	Enabled
72	vdom_link11	vlan_112A*	192.168.140.22/32	N/A	192.168.112.22/32	tcp_22 tcp_443	N/A	OP-32	2023_07_27T00:00	accept	Enabled
86	vdom_link11	vlan_112A*	192.168.140.50/32	N/A	192.168.112.50/32	tcp_443	N/A	OP-62	2023_07_20T00:00	accept	Enabled
87	vlan_112A*	vdom_link11	192.168.112.50/32	N/A	192.168.140.50/32	tcp_443	N/A	OP-62	2023_07_20T00:00	accept	Enabled
88	vdom_link11	vlan_112A*	192.168.50.50/32	N/A	192.168.112.50/32	tcp_443	N/A	OP-63	2023_07_20T00:00	accept	Enabled
89	vlan_112A*	vdom_link11	192.168.112.50/32	N/A	192.168.50.50/32	tcp_443	N/A	OP-63	2023_07_20T00:00	accept	Enabled
93	any	any	7.7.7.32	N/A	8.8.8.8/32 9.9.9.9/32	tcp_78 tcp_87	N/A	OP-167	2023_07_20T00:00	accept	Enabled
94	any	any	8.8.8.8/32	N/A	7.7.7.32 9.9.9.9/32	tcp_78 tcp_87	N/A	OP-167OP-170	2023_07_20T00:00	accept	Enabled


 Palo_Alto_1 # Expired Rules: 35 | Total Rules: 386

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
OP-351	untrust	test_db	192.168.83.25_32 192.168.73.25_32	N/A	192.168.140.25_32	tcp_25	any	OP-351-OP-362-OP-389-OP-410	2023_08_16T00_00	accept	Enabled
OP-352	untrust	test_db	192.168.50.25_32	N/A	192.168.140.25_32	tcp_25	any	OP-352	2023_08_16T00_00	accept	Enabled
OP-363	untrust	test_db	192.168.83.26_32 192.168.73.26_32	N/A	192.168.140.26_32	tcp_445 udp_445	any	OP-363-OP-372	2023_08_09T00_00	accept	Enabled
OP-383	untrust	test_db	192.168.83.27_32 10.0.0.27_32	N/A	192.168.140.27_32	tcp_80 tcp_23	any	OP-383	2023_08_09T00_00	accept	Enabled
OP-384	untrust	test_db	192.168.50.27_32	N/A	192.168.140.27_32	tcp_80 tcp_23	any	OP-384	2023_08_09T00_00	accept	Enabled
OP-390	untrust	test_db	192.168.83.25_32 192.168.73.25_32 10.0.0.25_32	N/A	192.168.140.25_32	tcp_445 tcp_443	any	OP-390-OP-410	2023_08_09T00_00	accept	Enabled
OP-455-1	untrust	test_db	192.168.50.26_32	N/A	192.168.140.26_32	tcp_445 udp_445	any	OP-455-1	2023_08_09T00_00	accept	Enabled
OP-467	any	any	55.55.55.32 5.5.5.32	N/A	66.66.66.66_32	tcp_55660 udp_55560	any	OP-467-OP-469OP-470OP-471	2023_08_16T00_00	accept	Enabled
OP-598	any	any	5.5.5.32 1.1.1.1	N/A	6.6.6.6_32 fw.com	tcp_445 tcp_446 tcp_80	any	OP-598-OP-172-OP-453-OP-461...	2023_08_25T00_00	accept	Enabled
OP-609-1	untrust	test_db	10.0.0.10_32	N/A	192.168.140.20_32	tcp_444 tcp_443	any	OP-609-1	2023_08_16T00_00	accept	Enabled
OP-659	any	any	5.5.5.32	N/A	6.6.6.6_32	tcp_80 tcp_81	any	OP-659	2023_09_10T00_00	accept	Enabled
OP-705-1	untrust	test_db	10.0.0.20_32	N/A	192.168.140.20_32	tcp_444 tcp_443	any	OP-705-1	2023_08_16T00_00	accept	Enabled
OP-68	test_db	untrust	192.168.140.155_32	N/A	192.168.50.10_32	udp_445	any	OP-68	2023_09_22T00_00	accept	Enabled
OP-724-1	test_db	untrust	192.168.140.20_32	N/A	192.168.112.20_32	tcp_444 tcp_443	any	OP-724-1	2023_08_16T00_00	accept	Enabled
OP-726	untrust	test_db	192.168.50.23_32 192.168.50.24_32 5.5.5.32	N/A	192.168.140.25_32	tcp_445 udp_445	any	OP-726-OP-729	2023_09_17T00_00	accept	Enabled
OP-735-1	untrust	test_db	10.0.0.21_32	N/A	192.168.140.20_32	tcp_444 tcp_443	any	OP-735-1	2023_08_16T00_00	accept	Enabled
OP-298	test_db	untrust	192.168.140.56_32	N/A	192.168.50.56_32	tcp_56	any	OP-298	2023_09_26T00_00	accept	Enabled
OP-309	test_db	untrust	192.168.140.15_32	N/A	192.168.50.15_32	tcp_1515	any	OP-309	2023_09_26T00_00	accept	Enabled
OP-313	test_db	untrust	192.168.140.33_32	N/A	192.168.50.33_32	tcp_443	any	OP-313	2023_09_27T00_00	accept	Enabled
OP-372	untrust test_ui	test_db	192.168.50.15_32 192.168.40.15_32	N/A	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	udp_445 udp_88 udp_389 tcp_53 tcp_445	any	OP-372	2023_09_27T00_00	accept	Enabled


 FG_Opinntate_2 | root # Expired Rules: 12 | Total Rules: 167


Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
126	any	any	8.8.8.8/32	N/A	7.7.7.7/32	tcp_78 tcp_87	N/A	OP-167	2023_07_20T00:00	accept	Enabled
50	port1	vdom_link10	192.168.30.222/32	N/A	192.168.112.222/32	tcp_443 tcp_80	N/A	differentcomment	2023_06_30T00:00	accept	Enabled
54	port1	vdom_link10	192.168.140.12/32	N/A	192.168.112.12/32	tcp_443	N/A	test	2023_07_26T00:00	accept	Enabled
55	vdom_link10	port1	192.168.112.12/32	N/A	192.168.140.12/32	tcp_443	N/A	test	2023_07_26T00:00	accept	Enabled
80	port1	vdom_link10	192.168.140.12/32	N/A	192.168.112.12/32	tcp_444	N/A	OP-26	2023_07_20T00:00	accept	Enabled
92	port1	vdom_link10	192.168.140.22/32	N/A	192.168.112.22/32	tcp_22 tcp_443	N/A	OP-32	2023_07_27T00:00	accept	Enabled
108	port1	vdom_link10	192.168.140.50/32 1.1.12.0/24	N/A	192.168.112.50/32	tcp_443	N/A	OP-62	2023_07_20T00:00	accept	Enabled
109	vdom_link10	port1	192.168.112.50/32	N/A	192.168.140.50/32	tcp_443	N/A	OP-62	2023_07_20T00:00	accept	Enabled
110	port1	vdom_link10	192.168.50.50/32 192.168.50.97/32	N/A	192.168.112.50/32 192.168.50.75/32	tcp_443	N/A	OP-63OP-4432ankara	2023_07_20T00:00	accept	Enabled
111	vdom_link10	port1	192.168.112.50/32	N/A	192.168.50.50/32	tcp_443	N/A	OP-63	2023_07_20T00:00	accept	Enabled


123	any	any	7.7.7.7/32	N/A	8.8.8.8/32	tcp_78 tcp_87	N/A	OP-167	2023_07_20T00:00	accept	Enabled
124	any	any	8.8.8.8/32	N/A	7.7.7.7/32	tcp_78 tcp_87	N/A	OP-167	2023_07_20T00:00	accept	Enabled

 PaloAlto_2 # Expired Rules: 9 | Total Rules: 66

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
usom-1	any	any	fortiguard usom	N/A	2.2.2.2_32 8.8.8.8_32	tcp_12 tcp_21 tcp_89 tcp_98 udp_89 udp_98	any	Opinnate131testOP-483	2023_07_22T00_00	accept	Enabled
OP-17-1	any	any	9.9.9.9_32	N/A	2.2.2.2_32	tcp_89 tcp_98 udp_89 udp_98 tcp_12 tcp_21	any	a1b2aniil3-CANCAN-OP-254	2023_07_22T00_00	accept	Enabled
OP-524	external	prod_db	192.168.40.40_32	N/A	192.168.132.137_32	tcp_555	any	OP-524OP-529OP-531	2023_08_30T00_00	accept	Enabled
OP-372	external	prod_app	192.168.50.15_32 192.168.40.15_32	N/A	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	udp_445 udp_88 udp_389 tcp_53 tcp_445	any	OP-372	2023_09_27T00_00	accept	Enabled
OP-372-i	external	prod_app	192.168.50.15_32 192.168.40.15_32	N/A	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	any	icmp	OP-372	2023_09_27T00_00	accept	Enabled
OP-372-1	prod_app	external	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	N/A	192.168.50.15_32 192.168.40.15_32	udp_445 udp_88 udp_389 tcp_53 tcp_445	any	OP-372	2023_09_27T00_00	accept	Enabled
OP-372-1-i	prod_app	external	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	N/A	192.168.50.15_32 192.168.40.15_32	any	icmp	OP-372	2023_09_27T00_00	accept	Enabled
OP-387-i	any	any	192.168.140.10_32	N/A	any 9.9.9.9_32	any	icmp	OP-387-OP-469-OP-470	2023_09_26T12_52	accept	Enabled
OP-643-i	prod_db	external	192.168.132.155_32	N/A	192.168.50.11_32	any	icmp	OP-643	2023_10_04T00_00	accept	Enabled


 cp-2sms | vs_3rd_party
No Data

 cp-sms2 | vs_opinnate
No Data

 cp-sms1 | cp-node
No Data

 PA3000-OP3 # Expired Rules: 5 | Total Rules: 28

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
OP-372	untrust	cp_spark_zone	192.168.50.15_32 192.168.40.15_32	N/A	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	udp_445 udp_88 udp_389 tcp_53 tcp_445	any	OP-372	2023_09_27T00_00	accept	Enabled
OP-372-i	untrust	cp_spark_zone	192.168.50.15_32 192.168.40.15_32	N/A	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	any	icmp	OP-372	2023_09_27T00_00	accept	Enabled
OP-372-1	cp_spark_zone	untrust	192.168.83.30_32 192.168.69.71_32	N/A	192.168.50.15_32 192.168.40.15_32 192.168.180.17_32	udp_445 udp_88 udp_389 tcp_53 tcp_445	any	OP-372--OP-5752	2023_09_27T00_00	accept	Enabled
OP-372-1-i	cp_spark_zone	untrust	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	N/A	192.168.50.15_32 192.168.40.15_32	any	icmp	OP-372	2023_09_27T00_00	accept	Enabled
OP-5976	any	any	192.168.133.10_32	N/A	192.168.83.86_32	tcp_3389	any	OP-5976	2023_11_09T00_00	accept	Enabled

 PA-Opinnate-v9
No Data

Permissive Rule Usage on Firewalls

Permissive rules with critical or high degree meaning allowing thousands of IP addresses or big spectrum of services must be avoided. Here is the list of first 20 rules on each firewall that are permissive rules.

Permissive High Rules

Permissive High Rules	41
Total Rules	1217


 cp_cluster | cp-cluster

No Data


 FG_Opinnate_1 # Permissive High Rules: 27 | Total Rules: 453

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
4	any	any	192.168.8.70/32 192.168.9.71-192.168.9.103	N/A	192.168.13.8/32	tcp_99-195 tcp_66 ALL_ICMP udp_73 NFS	N/A		always	accept	Enabled
14	sd-wan3	sd-wan2	192.168.99.0/24 224.0.0.0/16	N/A	192.168.25.0/24	tcp_443	N/A		always	accept	Enabled
33	any	any	192.168.13.8/32	N/A	192.168.8.70/32 192.168.9.71-192.168.9.103	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A		always	accept	Enabled
55	any	any	192.168.8.70/32 192.168.9.71-192.168.9.103	ldap_grp admanil CN=10b3ad2a-6883-4fa7-90...	192.168.13.8/32	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A		always	accept	Enabled
101	any	any	192.168.8.70/32 192.168.9.71-192.168.9.103	oplocal\admmert oplocal\admanil	192.168.13.8/32	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A	SNSA-55	always	accept	Enabled
105	any	any	192.168.8.70/32 192.168.9.71-192.168.9.103	oplocal\admmert	192.168.112.0/24	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A	SNSA-55	always	accept	Enabled
103	any	any	192.168.8.70/32 192.168.9.71-192.168.9.103	oplocal\admmert	192.168.13.8/32	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A	SNSA-55	always	accept	Enabled
152	sd-wan3	sd-wan3	192.168.133.133/32 169.0.0.0-169.255.255.255	N/A	192.168.50.25/32	tcp_21342	N/A	test1	always	accept	Enabled
179	sd-wan3	sd-wan3	192.168.50.25/32	N/A	192.168.92.50/32	tcp_63 udp_90-10101	N/A	test1	always	accept	Enabled
180	sd-wan3	sd-wan3	192.168.92.50/32	N/A	192.168.50.25/32	tcp_63 udp_90-10101	N/A	test1	always	accept	Enabled
183	sd-wan3	sd-wan3	192.168.50.25/32	N/A	127.0.0.0/8 192.168.91.66/32 192.168.92.6/32	tcp_21 tcp_80	N/A	test1	always	accept	Enabled
239	any	any	192.168.16.5/32	N/A	192.168.0.0/16	tcp_21 udp_41 ALL_ICMP	N/A	OP-2094	always	accept	Enabled
242	any	any	192.168.63.6/32	N/A	192.168.0.0/15	tcp_55 ALL_ICMP	N/A	OP-2190	always	accept	Enabled
248	sd-wan2	sd-wan3	192.168.25.60/32	N/A	192.168.112.63/32	tcp_66 udp_32-69 ALL_ICMP	N/A	OP-2221	always	accept	Enabled
249	sd-wan3	sd-wan2	192.168.112.63/32	N/A	192.168.25.60/32	tcp_66 udp_32-69 ALL_ICMP	N/A	OP-2221	always	accept	Enabled
257	sd-wan3	sd-wan2	192.168.132.158/32 192.168.99.70/32 192.168.112.35/32	N/A	192.168.25.17/32	tcp_19-80 udp_50	N/A	OP-2258	always	accept	Enabled
366	any	any	192.168.82.36/32 192.168.112.36/32	N/A	192.168.112.63/32 192.168.69.88/32 192.168.28.0/28 192.168.17.0/24 192.168.25.69/32	tcp_57-168 udp_85-200 udp_53 tcp_53 tcp_80 tcp_443 ALL_ICMP	N/A	OP-2519	always	accept	Enabled
388	sd-wan2	sd-wan3	192.168.20.0/24	N/A	192.168.112.100-192.168.112.200 192.168.140.100-192.168.140.105 192.168.133.111/32 192.168.140.0/23	tcp_100 udp_100-200 ALL_ICMP	N/A	OP-102	always	accept	Enabled
572	sd-wan3 client_zone	any	192.168.40.0/24	N/A	192.168.0.0/24	tcp_1820 tcp_183 tcp_1842 tcp_1843 tcp_1846 tcp_1851 tcp_1852 tcp_1854 tcp_1856 tcp_1857 tcp_1864 tcp_1865 tcp_1866 tcp_1867 tcp_1872 tcp_1873 tcp_188 tcp_1883 tcp_1887 tcp_1891 tcp_1896 tcp_1902 tcp_1903 tcp_1905 tcp_1908	N/A	RU-OP-54-1941	always	accept	Enabled

571	sd-wan3 client_zone	any	192.168.40.0/24	N/A	192.168.0.0/24	tcp_1729 tcp_173 tcp_1735 tcp_1736 tcp_1738 tcp_174 tcp_1745 tcp_1751 tcp_1755 tcp_1757 tcp_1758 tcp_1763 tcp_1767 tcp_1768 tcp_1774 tcp_1791 tcp_1796 tcp_1799 tcp_1800 tcp_1801 tcp_1802 tcp_1807 tcp_1810 tcp_1813 tcp_1817	N/A	RU-OP-54-1940	always	accept	Enabled
-----	------------------------	-----	-----------------	-----	----------------	--	-----	---------------	--------	--------	---------

 FG_Opinnate_2 | Customer_vd


No Data

 Palo_Alto_1 # Permissive High Rules: 10 | Total Rules: 386


Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
OP-43	untrust	test_ui test_app	192.168.12.44_32	N/A	192.168.133.89_32 192.168.150.157_32	tcp_80 tcp_443 tcp_3125-5588	any	OP-43	always	accept	Enabled
OP-51	untrust	test_app linux_zone test_ui	192.168.8.70_32 192.168.9.71-192.168.9.100	N/A	192.168.150.17_32 192.168.170.55_32 192.168.133.14_32	tcp_99-195 tcp_66 udp_73 tcp_111 tcp_2049 udp_111 udp_2049	any	OP-51	always	accept	Enabled
OP-51-1	test_app linux_zone test_ui	untrust	192.168.150.17_32 192.168.170.55_32 192.168.133.14_32	N/A	192.168.8.70_32 192.168.9.71-192.168.9.100	tcp_99-195 tcp_66 udp_73	any	OP-51-1	always	accept	Enabled
OP-56	untrust	test_ui	192.168.8.70_32 192.168.9.71-192.168.9.100	N/A	192.168.133.26_32	tcp_99-195 tcp_66 udp_73 tcp_111 tcp_2049 udp_111 udp_2049	any	OP-56	always	accept	Enabled
OP-56-1	test_ui	untrust	192.168.133.26_32	N/A	192.168.8.70_32 192.168.9.71-192.168.9.100	tcp_99-195 tcp_66 udp_73	any	OP-56-1	always	accept	Disabled
OP-458-7	asa_zone test_ui test_db test_app test_app2 linux_zone	untrust linux_zone	any 192.168.170.48_32	N/A	172.145.21.3_32 172.23.36.39_32 172.35.68.69_32 192.168.170.48_32	tcp_445	any	OP-458-7	always	accept	Enabled
OP-458-9	untrust asa_zone test_ui test_db test_app test_app2 linux_zone	test_ui untrust linux_zone	any 192.168.170.48_32	N/A	192.168.133.9-192.168.133.49 192.168.98.66_32 192.168.95.63_32 172.35.68.69_32 192.168.170.48_32	tcp_66 tcp_42 tcp_21 tcp_43	any	OP-458-9-OP-474	always	accept	Enabled
OP-5875	untrust	test_db	192.168.0.0/16 192.168.50.11_32	N/A	192.168.140.11_32	tcp_443	any	OP-5875	always	accept	Enabled
OP-5883-11	untrust	test_db	192.168.0.0/16 192.168.120.10_32	N/A	192.168.140.53_32	udp_44	any	OP-5883-11	always	accept	Enabled
OP-5936	untrust	test_db	10.0.0.10_32	N/A	192.168.140.10_32	tcp_589 tcp_577 tcp_588 udp_789 udp_788 tcp_443 tcp_445 tcp_43 tcp_447 tcp_333 tcp_444 tcp_446 tcp_448 tcp_459 tcp_449 tcp_450 tcp_452 tcp_458 tcp_441 tcp_478 udp_443	any	OP-5936	always	accept	Enabled

 FG_Opinnate_2 | root # Permissive High Rules: 1 | Total Rules: 167


Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
113	port1	cp_net	192.168.132.156/32 192.168.30.13-192.168.30.43	N/A	192.168.83.50/32 9.9.9.9/32	tcp_50-100	N/A	OP-67OP-4420	always	accept	Enabled

 PaloAlto_2 # Permissive High Rules: 2 | Total Rules: 66

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
OP-43	external	prod_db	192.168.12.44_32	N/A	192.168.132.174_32	tcp_80 tcp_443 tcp_3125-5588	any	OP-43	always	accept	Enabled
OP-56	prod_db prod_app	external	any 192.168.170.15_32 192.168.140.15_32	N/A	192.168.133.26_32 192.168.112.25_32	tcp_99-195 tcp_66 udp_73	any	OP-56-cck1	always	accept	Enabled

 cp-2sms | vs_3rd_party

No Data

 cp-sms2 | vs_opinnate

No Data

No Data

PA3000-OP3 # Permissive High Rules: 1 | Total Rules: 28

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
OP-5975	fg1_zone	cp_spark_zone untrust	192.168.140.10_32	N/A	192.168.160.3_32 any	tcp_444	any	OP-5975	always	accept	Enabled

PA-Opinnate-v9

No Data

Permissive Critical Rules

Permissive Critical Rules	119
Total Rules	1217

cp_cluster | cp-cluster # Permissive Critical Rules: 1 | Total Rules: 12

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
11	any	any	any	N/A	cp-gateway1 cp-cluster	any	any		always	accept	Enabled

FG_Opinnate_1 # Permissive Critical Rules: 23 | Total Rules: 453

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
576	any	any	any	N/A	185.67.34.90/32 *.usom.gov.tr	HTTP HTTPS	N/A		always	accept	Enabled
1	any	any	https_eriYim_grp	N/A	any	HTTPS SSH	N/A	OP-58	always	accept	Enabled
611	any	any	10.34.128.0/23	N/A	10.0.0.0/8	any	N/A	OP-58Copyofhttps	always	accept	Enabled
98	any	any	any	oplocal\admalitest oplocal\admanil	192.168.13.8/32	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A		always	accept	Enabled
133	any	any	192.168.50.50/32	N/A	192.168.132.142/32	any	N/A	1641	always	accept	Enabled
174	sd-wan3	sd-wan3	192.168.50.25/32	N/A	192.168.92.16/32 192.168.92.53/32 127.0.0.0/8 192.168.91.66/32 192.168.92.6/32	any	N/A	test1	always	accept	Enabled
182	sd-wan3	sd-wan3	127.0.0.0/8 192.168.91.66/32 192.168.92.6/32	N/A	192.168.50.25/32	any	N/A	test1	always	accept	Enabled
194	any	any	192.168.135.135/32	N/A	192.168.133.5-192.168.133.65	any	N/A	OP-2089	always	accept	Enabled
228	any	any	host 75.75.75.75 192.168.25.97/32	N/A	host 75.75.75.75 192.168.25.97/32	any	N/A	OP-2150OP2150OP2150OP21500...	always	accept	Enabled
282	client_zone	sd-wan3	192.168.40.43/32	N/A	192.168.132.169/32	any	N/A	OP-3	always	accept	Enabled
341	any	any	forti_group 192.168.112.168/32	N/A	A_group_1	any	N/A	OP-2326OP2326OP-2542	always	accept	Enabled
372	any	any	host 75.75.75.75 192.168.25.97/32	N/A	host 75.75.75.75	any	N/A	OP-2604OP-2604OP-2604OP-260...	always	accept	Enabled
414	sd-wan3	sd-wan3	192.168.99.7/32	N/A	192.168.50.56/32 192.168.132.167/32 192.168.132.172/32 192.168.140.53/32	any	N/A	OP-2996	always	accept	Enabled
642	any	any	forti_group	N/A	A_grp_1	any	N/A	OP-2326	always	accept	Enabled
397	client_zone	sd-wan3	192.168.40.42/32	N/A	10.0.0.10/32	any	N/A	OP-476	always	accept	Enabled
431	client_zone port3	sd-wan3 client_zone port3	192.168.40.10/32 192.168.50.10/32	N/A	192.168.40.10/32 192.168.50.10/32	any	N/A	OP-145CopyofOP-145-1	always	accept	Disabled
454	sd-wan3 client_zone port3 port4	any	192.168.40.0/24	N/A	any	DNS HTTP HTTPS FTP	N/A	OP-628	always	accept	Disabled
467	any	sd-wan3	any	N/A	192.168.150.17/32 192.168.133.14/32	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A	OP-51	always	accept	Enabled
581	any	sd-wan3	any	N/A	192.168.133.26/32 192.168.112.25/32	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A	OP-56	always	accept	Enabled
487	any	any	10.0.0.110/32	N/A	192.168.160.0/24	any	N/A	cpsms-spark	always	accept	Enabled

FG_Opinnate_2 | Customer_vd # Permissive Critical Rules: 5 | Total Rules: 96

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
33	vdom_link11	vlan_112A°	192.168.73.73/32	N/A	192.168.112.0/24	any	N/A	OP-84	always	accept	Enabled
69	vlan_112A° vdom_link11	vdom_link11 vlan_112A°	192.168.112.50/32 1.3.3.3/32 192.168.99.50/32	N/A	192.168.50.50/32 192.168.30.30/32 1.3.3.3/32 192.168.99.50/32 192.168.112.50/32	any	N/A	OP-4342	always	accept	Enabled
68	vlan_112A° vdom_link11	vdom_link11 vlan_112A°	192.168.112.50/32 192.168.99.50/32	N/A	192.168.50.50/32 192.168.30.30/32 192.168.99.50/32 192.168.112.50/32	any	N/A	OP-4342	always	accept	Enabled
62	vlan_112A°	vdom_link11	192.168.112.50/32 192.168.112.36/32 192.168.112.85/32 192.168.112.92/32 192.168.112.53/32 192.168.112.126/32	N/A	192.168.99.50/32	any	N/A	OP-4342	always	accept	Enabled
61	vdom_link11	vlan_112A°	192.168.99.50/32	N/A	192.168.112.58/32 192.168.112.112/32	any	N/A	OP-4342	always	accept	Enabled

Palo_Alto_1 # Permissive Critical Rules: 42 | Total Rules: 386

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
ipsec	any	any	10.34.128.201 10.34.128.203	N/A	10.34.128.201 10.34.128.203	any	any		always	accept	Enabled
OP-295-3-i	untrust	test_db test_ui	192.168.50.73_32	N/A	192.168.133.121_32 192.168.140.53_32	any	icmp	OP-295-3-OP-57-OP-5276	always	accept	Enabled
OP-295-7-i	untrust	test_ui	192.168.50.73_32	N/A	192.168.133.126_32	any	icmp	OP-295-7	always	accept	Enabled

OP-4990-i	any	any	rev_test	N/A	192.168.50.134_32	any	icmp		always	accept	Enabled
commen-Policy-i	asa_zone	test_ui	192.168.170.15_32 192.168.170.16_32 192.168.170.24_32	N/A	192.168.180.17_32	any	icmp	commen-Policy-OP-32	always	accept	Enabled
OP-51-1-i	test_app linux_zone test_ui	untrust	192.168.150.17_32 192.168.170.55_32 192.168.133.14_32	N/A	192.168.8.70_32 192.168.9.71-192.168.9.100	any	icmp	OP-51-1	always	accept	Enabled
OP-51-3	untrust asa_zone test_ui test_db test_app test_app2 linux_zone	test_app test_ui linux_zone	any	N/A	192.168.150.17_32 192.168.133.14_32 192.168.170.55_32	tcp_99-195 tcp_66 udp_73	any	OP-51-3	always	accept	Enabled
OP-51-3-i	untrust asa_zone test_ui test_db test_app test_app2 linux_zone	test_app test_ui linux_zone	any	N/A	192.168.150.17_32 192.168.133.14_32 192.168.170.55_32	any	icmp	OP-51-3	always	accept	Enabled
OP-51-i	untrust	test_app linux_zone test_ui	192.168.8.70_32 192.168.9.71-192.168.9.100	N/A	192.168.150.17_32 192.168.170.55_32 192.168.133.14_32	any	icmp	OP-51OP-356OP-357	always	accept	Enabled
OP-56-i	untrust	test_ui	192.168.8.70_32 192.168.9.71-192.168.9.100	N/A	192.168.133.26_32	any	icmp	OP-56OP-356OP-357	always	accept	Enabled
OP-56-1-i	test_ui	untrust	192.168.133.26_32	N/A	192.168.8.70_32 192.168.9.71-192.168.9.100	any	icmp	OP-56-1	always	accept	Enabled
OP-56-3	untrust asa_zone test_ui test_db test_app test_app2 linux_zone	test_ui untrust	any	N/A	192.168.133.26_32 192.168.112.25_32	tcp_99-195 tcp_66 udp_73	any	OP-56-3	always	accept	Enabled
OP-56-3-i	untrust asa_zone test_ui test_db test_app test_app2 linux_zone	test_ui untrust	any	N/A	192.168.112.25_32	any	icmp	OP-56-3-OP-628	always	accept	Enabled
OI-22-i	any	any	192.168.23.26_32	N/A	192.168.25.36_32 192.168.16.17_32 192.168.17.18_32	any	icmp	OI-22-OP-6008	always	accept	Enabled
OP-5230-i	any	any	192.168.36.29_32	N/A	168.27.15.48_32	any	icmp	OP-5230	always	accept	Enabled
OP-5230-1-i	any	any	192.168.36.29_32	N/A	168.27.15.48_32	any	icmp	OP-5230-1	always	accept	Enabled
OP-66-i	any	any	234.213.121.12_32	N/A	123.123.22.22_32	any	icmp	OP-66	always	accept	Enabled
OP-5425-i	any	any	192.168.73.10_32 172.35.68.69_32	N/A	192.168.83.10_32 172.35.68.69_32 192.168.67.10_32	any	icmp	ali-replace-OP-5730-OP-632...	always	accept	Enabled
OP-276-i	untrust	test_ui	192.168.93.10_32	N/A	192.168.133.33_32	any	icmp	OP-276	always	accept	Enabled
OP-5604	untrust	test_ui	192.168.112.48_32 192.168.120.66_32	N/A	192.168.133.123_32	any	any	OP-5604	always	accept	Enabled


 FG_Opinntate_2 | root # Permissive Critical Rules: 10 | Total Rules: 167

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
18	port1 cp_net port2	cp_net port1	10.0.0.110 10.0.0.111 178.157.15.222/32	N/A	10.0.0.110 10.0.0.111 178.157.15.222/32	any	N/A	OP-59	always	accept	Enabled
125	cp_net port2	port1 cp_net port2	10.0.0.110 10.0.0.111 10.0.0.112	N/A	any	any	N/A	Reverseof1	always	accept	Enabled
1	port1 cp_net port2	cp_net port2	any	N/A	10.0.0.110 10.0.0.111 10.0.0.112	any	N/A		always	accept	Enabled
31	cp_net	port1 vdom_link10	192.168.73.73/32	N/A	3.3.3.3/32 1.3.3.3/32 192.168.50.50/32 192.168.30.30/32 192.168.93.0/24 192.168.112.0/24 192.168.5.5/32	any	N/A	OP-84	always	accept	Enabled
81	port1	vdom_link10	192.168.99.50/32	N/A	192.168.112.58/32 192.168.112.112/32	any	N/A	OP-4342	always	accept	Enabled
82	vdom_link10 port1	port1	192.168.112.50/32 178.157.15.29/32 192.168.112.36/32 192.168.112.85/32 192.168.112.92/32 192.168.112.53/32 192.168.112.126/32	N/A	192.168.99.50/32	any	N/A	OP-4342	always	accept	Enabled
88	vdom_link10 port1	port1 vdom_link10	192.168.112.50/32 192.168.99.50/32	N/A	192.168.50.50/32 192.168.30.30/32 192.168.99.50/32 192.168.112.50/32	any	N/A	OP-4342	always	accept	Enabled
89	vdom_link10 port1	port1 vdom_link10	192.168.112.50/32 1.3.3.3/32 192.168.99.50/32	N/A	192.168.50.50/32 192.168.30.30/32 1.3.3.3/32 192.168.99.50/32 192.168.112.50/32	any	N/A	OP-4342	always	accept	Enabled
52	any	any	any	N/A	185.67.34.90 usom.gov.tr	any	N/A		always	accept	Enabled
121	any	any	any	N/A	178.157.15.246	HTTP HTTPS SSH TELNET	N/A	fwerisim	always	accept	Enabled


 PaloAlto_2 # Permissive Critical Rules: 30 | Total Rules: 66

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
OP-295-3-i	external	prod_db	192.168.50.73_32	N/A	192.168.132.188_32 192.168.132.181_32	any	icmp	revreplaceComment	always	accept	Enabled
OP-295-5-i	external	prod_db	192.168.50.73_32	N/A	192.168.132.169_32	any	icmp	aas	always	accept	Enabled
commen-Policy-i	external	prod_db	192.168.170.15_32 192.168.170.16_32 192.168.170.24_32	N/A	192.168.180.17_32	any	icmp	commen-Policy-OP-32	always	accept	Enabled
OP-51	prod_db prod_app	external	any	N/A	192.168.150.17_32 192.168.170.55_32 192.168.133.14_32	tcp_99-195 tcp_66 udp_73	any	OP-51	always	accept	Enabled
OP-51-i	prod_db prod_app	external	192.168.140.50_32 2.2.2.2_32	N/A	192.168.150.17_32 192.168.170.55_32 192.168.133.14_32	any	icmp	OP-51-	always	accept	Enabled
OP-56-i	prod_db prod_app	external	any 192.168.170.15_32 192.168.140.15_32 192.168.40.41_32 192.168.83.83-192.168.83.90	N/A	192.168.133.26_32 192.168.112.25_32	any	icmp	OP-56-cck1--cck2	always	accept	Enabled
OI-22-i	any	any	192.168.23.26_32	N/A	192.168.25.36_32	any	icmp	OI-22	always	accept	Disabled
OP-5230-i	any	any	192.168.36.29_32	N/A	168.27.15.48_32	any	icmp	OP-5230	always	accept	Enabled
OP-5273	any	any	192.168.73.10_32	N/A	192.168.132.128_25	any	any	OP-5273Test-1	always	accept	Enabled
OP-5273-1	any	any	192.168.132.128_25 192.168.40.41_32 192.168.83.83-192.168.83.90	N/A	192.168.73.10_32 172.16.2.0_24	any	any	OP-5273Test-1--cck2-v-cck4...	always	accept	Enabled

OP-5420-i	any	any	44.41.2.4_32 192.168.25.36_32 172.35.68.69_32 192.168.16.17_32 192.168.17.18_32	N/A	12.3.31.4_32 192.168.25.36_32 172.35.68.69_32 172.16.2.0_24 192.168.20.23_32 192.168.132.130_32 192.168.16.17_32 192.168.17.18_32	any	icmp	ali-replace-vs-cck4-OP-5730...	always	accept	Enabled
OP-5425-i	any	any	192.168.73.10_32 172.35.68.69_32	N/A	192.168.83.10_32 192.168.98.66_32 192.168.95.63_32 172.35.68.69_32 192.168.132.150_32 192.168.67.10_32	any	icmp	ali-replaceu--OP-5730-OP-632	always	accept	Enabled
OP-5604	external	prod_app	192.168.112.48_32 192.168.120.66_32	N/A	192.168.52.63_32	any	any	OP-5604	always	accept	Enabled
OP-5608	external	prod_app	192.168.120.36_32 192.168.133.26_32 192.168.40.41_32 192.168.83.83-192.168.83.90	N/A	192.168.52.63_32	any	any	OP-5608--cck2	always	accept	Enabled
OP-372-i	external	prod_app	192.168.50.15_32 192.168.40.15_32	N/A	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	any	icmp	OP-372	2023_09_27T00_00	accept	Enabled
OP-372-1-i	prod_app	external	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	N/A	192.168.50.15_32 192.168.40.15_32	any	icmp	OP-372	2023_09_27T00_00	accept	Enabled
OP-387	any	any	192.168.50.67_32	N/A	any	udp_342	any	OP-387	2023_09_26T12_52	accept	Disabled
OP-387-i	any	any	192.168.140.10_32	N/A	any 9.9.9.9_32	any	icmp	OP-387-OP-469-OP-470	2023_09_26T12_52	accept	Enabled
OP-387-1	any	any	any	N/A	192.168.50.67_32	udp_342	any	OP-387	2023_09_26T12_52	accept	Disabled
OP-387-1-i	any	any	any	N/A	192.168.50.67_32	any	icmp	OP-387	2023_09_26T12_52	accept	Disabled

 cp-2sms | vs_3rd_party

No Data

 cp-sms2 | vs_opinnate


No Data

 cp-sms1 | cp-node # Permissive Critical Rules: 1 | Total Rules: 9

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
8	any	any	any	N/A	cp-node	ssh_version_2 ssh echo-reply echo-request https	any		always	accept	Enabled

 PA3000-OP3 # Permissive Critical Rules: 7 | Total Rules: 28









Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
cp-sms-spark	cp_spark_zone fg1_zone	cp_spark_zone fg1_zone	10.0.0.110 cp-192.168.160.1	N/A	10.0.0.110 cp-192.168.160.1	any	any		always	accept	Enabled
cp-spark-erisim	untrust	any	op-net-10.34.128.0_23	N/A	any	any	any	OP-288OP-289	always	accept	Enabled
OP-372-i	untrust	cp_spark_zone	192.168.50.15_32 192.168.40.15_32	N/A	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	any	icmp	OP-372	2023_09_27T00_00	accept	Enabled
OP-372-1-i	cp_spark_zone	untrust	192.168.30.30_32 192.168.83.30_32 192.168.69.71_32	N/A	192.168.50.15_32 192.168.40.15_32	any	icmp	OP-372	2023_09_27T00_00	accept	Enabled
OP-458	untrust cp_spark_zone	untrust	any	N/A	172.145.21.3_32 172.35.68.69_32	tcp_445	any	test	always	accept	Enabled
OP-458-1	untrust cp_spark_zone	untrust fg1_zone	any	N/A	172.168.36.23_32 192.168.133.9-192.168.133.49 172.35.68.69_32	tcp_66 tcp_42 tcp_21 tcp_43	any	testupdate	always	accept	Enabled
OP-608	untrust	cp_spark_zone	192.168.120.10_32	N/A	any	tcp_444	any	OP-608	always	accept	Enabled

 PA-Opinnate-v9

No Data

Software Version Status

Outdated software version usage must be avoided. Here is the list of firewalls that are outdated.

Device Name	Device Ip	Version	Reason
 cp_cluster # cp-cluster	10.0.0.111	R81.20	No Version Information
 FG_Opinname_2 # Customer_vd	10.34.128.202	5.6.12	Outdated Version
 FG_Opinname_2 # root	10.34.128.202	5.6.12	Outdated Version
 PaloAlto_2	10.34.128.204	10.0.0	Outdated Version
 cp-2sms # vs_3rd_party	5.5.5.5		No Version Information
 cp-sms2 # vs_opinnate	6.6.6.6		No Version Information
 cp-sms1 # cp-node	10.0.0.112	R81.20	No Version Information
 PA-Opinnate-v9	10.34.128.185	9.0.1	Outdated Version

Corporate Security Policy Compliance

Rules must be compliant to the corporate security policy. Here is the list of first 20 rules on each firewall that are non-compliant.

Deny Rule	10
Total Rules	1217



cp_cluster | cp-cluster # Deny Rule: 1 | Total Rules: 12

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
2	any	any	10.0.0.100	N/A	10.115.207.100	Tcp_3389 tcp_3389	any	OP-5995	101123T0000	accept	Enabled



FG_Opinrate_1 # Deny Rule: 7 | Total Rules: 453

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
588	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32 10.0.0.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 192.168.170.53/32 1.1.1.1/32 10.0.0.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5936	always	accept	Enabled
597	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32 10.0.0.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 192.168.170.53/32 1.1.1.1/32 10.0.0.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5936	always	accept	Enabled
598	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32 10.0.0.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 192.168.170.53/32 1.1.1.1/32 10.0.0.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5936	always	accept	Enabled
601	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32 10.0.0.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 192.168.170.53/32 1.1.1.1/32 10.0.0.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5936	always	accept	Enabled
602	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32 10.0.0.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 192.168.170.53/32 1.1.1.1/32 10.0.0.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5936	always	accept	Enabled
603	sd-wan3 port3 client_zone	client_zone sd-wan3 port3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 192.168.170.53/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32 10.0.0.10/32	N/A	192.168.40.10/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 192.168.170.53/32 1.1.1.1/32 10.0.0.10/32 192.168.50.10/32 192.168.50.11/32	tcp_21	N/A	OP-5936	always	accept	Enabled
712	sd-wan3 port3 client_zone	client_zone port3 sd-wan3	192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.50.10/32 1.1.1.1/32 192.168.40.10/32 192.168.50.11/32 192.168.120.10/32 10.0.0.10/32 192.168.140.10/32	N/A	192.168.40.10/32 192.168.50.10/32 192.168.50.11/32 192.168.112.92/32 192.168.112.126/32 192.168.112.53/32 192.168.120.10/32 10.0.0.10/32 192.168.140.10/32	tcp_21	N/A	OP-5975	always	accept	Enabled



FG_Opinrate_2 | Customer_vd

No Data



Palo_Alto_1 # Deny Rule: 1 | Total Rules: 386

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
OP-85	untrust	test_db	10.0.0.20_32	N/A	192.168.140.20_32 10.0.0.22_32	tcp_80	any	OP-85-OP-91	always	accept	Enabled



FG_Opinrate_2 | root # Deny Rule: 1 | Total Rules: 167

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
125	cp_net port2	port1 cp_net port2	10.0.0.110 10.0.0.111 10.0.0.112	N/A	any	any	N/A	Reverseof1	always	accept	Enabled




PaloAlto_2


No Data





cp-2sms | vs_3rd_party

No Data

 cp-sms2 | vs_opinnate
No Data

 cp-sms1 | cp-node
No Data

 PA3000-OP3
No Data

 PA-Opinnate-v9
No Data

Existing Firewall Topology

Overall device topology for the devices added to the system can be found in this section as below.

There is no topology map. Please save it first.

Comment Usage on The Rules

Each rule must have a reason statement or ticket reference about the need. Here is the list of first 20 rules on each firewall that are not containing reason or ticket reference.

No Comment Rules	33
Total Rules	1217



cp_cluster | cp-cluster # No Comment Rules: 2 | Total Rules: 12

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
12	any	any	any	N/A	any	any	any		always	deny	Enabled
11	any	any	any	N/A	cp-gateway1 cp-cluster	any	any		always	accept	Enabled



FG_Opinntate_1 # No Comment Rules: 17 | Total Rules: 453

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
608	palo	sd-wan3	1.3.3.3/32	N/A	10.10.10.11/32	ALL_ICMP	N/A		always	accept	Enabled
576	any	any	any	N/A	185.67.34.90/32 *.usom.gov.tr	HTTP HTTPS	N/A		always	accept	Enabled
4	any	any	192.168.8.70/32 192.168.9.71-192.168.9.103	N/A	192.168.13.8/32	tcp_99-195 tcp_66 ALL_ICMP udp_73 NFS	N/A		always	accept	Enabled
9	any	any	172.16.2.33	N/A	exclude_private_net	any	N/A		always	accept	Enabled
11	any	any	client 0/8_network 127.0.0.0/8	N/A	forti_4 172.16.0.0/12 192.168.0.0/16	tcp_80 ALL_ICMP	N/A		always	accept	Enabled
14	sd-wan3	sd-wan2	192.168.99.0/24 224.0.0.0/16	N/A	192.168.25.0/24	tcp_443	N/A		always	accept	Enabled
15	sd-wan3	sd-wan3	192.168.94.0/27	N/A	172.16.2.36/32	tcp_33 udp_22	N/A		always	accept	Enabled
17	sd-wan3	sd-wan3	172.16.2.37/32	N/A	192.168.94.68/32	tcp_66	N/A		always	accept	Enabled
33	any	any	192.168.13.8/32	N/A	192.168.8.70/32 192.168.9.71-192.168.9.103	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A		always	accept	Enabled
55	any	any	192.168.8.70/32 192.168.9.71-192.168.9.103	ldap_grp admanil CN=10b3ad2a-6883-4fa7-90...	192.168.13.8/32	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A		always	accept	Enabled
80	any	any	A_group_1	N/A	B_grp_2	tcp_222	N/A		always	accept	Enabled
82	any	any	A_group_1	CN=293f0798-ea5c-4455-9f...	B_grp_2	udp_11	N/A		always	accept	Enabled
83	any	any	A_group_1 192.168.13.8/32	N/A	B_grp_2	tcp_11	N/A		always	accept	Enabled
84	any	any	A_grp	N/A	X_grp	tcp_443 tcp_79 udp_79	N/A		always	accept	Enabled
85	any	any	A_group_1	N/A	B_grp_2	tcp_443 tcp_79 udp_79	N/A		always	accept	Enabled
98	any	any	any	oplocal\admalitest oplocal\admanil	192.168.13.8/32	tcp_99-195 tcp_66 ALL_ICMP udp_73	N/A		always	accept	Enabled
453	port3	client_zone	192.168.50.10/32	N/A	192.168.40.10/32	HTTPS	N/A		always	accept	Disabled



FG_Opinntate_2 | Customer_vd # No Comment Rules: 2 | Total Rules: 96

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
2	port6	vlan_112A*	50.50.50.50/32	N/A	autoupdate.opera.com	HTTP HTTPS	N/A		always	accept	Enabled
7	port6	vlan_112A*	any	N/A	any	any	N/A		always	deny	Enabled



Palo_Alto_1 # No Comment Rules: 6 | Total Rules: 386

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
ipsec	any	any	10.34.128.201 10.34.128.203	N/A	10.34.128.201 10.34.128.203	any	any		always	accept	Enabled
OP-4973-3	any	any	rev_test	N/A	192.168.50.23_32	tcp_443	any		always	accept	Enabled
OP-4974	any	any	rev_test	N/A	192.168.50.99_32	tcp_331	any		always	accept	Enabled
OP-4979	any	any	rev_test	N/A	palo_group	tcp_2243 tcp_7897	any		always	accept	Enabled
OP-4990-i	any	any	rev_test	N/A	192.168.50.134_32	any	icmp		always	accept	Enabled
OP-37	any	any	forDecommi	N/A	192.168.47.23_32	tcp_999 udp_51	any		always	accept	Enabled



FG_Opinntate_2 | root # No Comment Rules: 3 | Total Rules: 167

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
1	port1 cp_net port2	cp_net port2	any	N/A	10.0.0.110 10.0.0.111 10.0.0.112	any	N/A		always	accept	Enabled
52	any	any	any	N/A	185.67.34.90 usom.gov.tr	any	N/A		always	accept	Enabled
146	any	any	192.148.8.70/32	N/A	192.118.13.8/32	udp_10010	N/A		always	accept	Enabled



PaloAlto_2

No Data



cp-2sms | vs_3rd_party

No Data



cp-sms2 | vs_opinnate

No Data



cp-sms1 | cp-node # No Comment Rules: 2 | Total Rules: 9

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
9	any	any	any	N/A	any	any	any		always	deny	Enabled
8	any	any	any	N/A	cp-node	ssh_version_2 ssh echo-reply echo-request https	any		always	accept	Enabled



PA3000-OP3 # No Comment Rules: 1 | Total Rules: 28

Rule Id	From	To	Source	Users	Destination	Service	Application	Comment	Schedule	Action	Status
cp-sms-spark	cp_spark_zone fg1_zone	cp_spark_zone fg1_zone	10.0.0.110 cp-192.168.160.1	N/A	10.0.0.110 cp-192.168.160.1	any	any		always	accept	Enabled



PA-Opinnate-v9

No Data

Admin Users on The System

Default username and passwords must be changed and not used. Here is the list of admin users on each firewall.



cp_cluster | cp-cluster

Admin Name	Remote Auth Profile	User Type	User Role
admin (default admin user)		local	['Web-UI', 'CLI', 'Gaia-API']
monitor		local	['Web-UI', 'CLI', 'Gaia-API']



FG_Opinname_1

Admin Name	Remote Auth Profile	User Type	User Role
admanil	oplocal_az_admins	remote_user	super_admin
admcanx	oplocal_radius	remote_user	super_admin
admin (default admin user)		local	super_admin



FG_Opinname_2 | Customer_vd

Admin Name	Remote Auth Profile	User Type	User Role
admin (default admin user)		local	super_admin
opinnate		local	super_admin



Palo_Alto_1

Admin Name	Remote Auth Profile	User Type	User Role
admin (default admin user)		local	superuser



FG_Opinname_2 | root

Admin Name	Remote Auth Profile	User Type	User Role
admin (default admin user)		local	super_admin
opinnate		local	super_admin



PaloAlto_2

Admin Name	Remote Auth Profile	User Type	User Role
admin (default admin user)		local	superuser



cp-2sms | vs_3rd_party

No Data



cp-sms2 | vs_opinnate

No Data



cp-sms1 | cp-node

Admin Name	Remote Auth Profile	User Type	User Role
admin (default admin user)		local	['Web-UI', 'CLI', 'Gaia-API']
monitor		local	['Web-UI', 'CLI', 'Gaia-API']



PA3000-OP3

Admin Name	Remote Auth Profile	User Type	User Role
admin (default admin user)		local	superuser



PA-Opinnate-v9

No Data