Cisco Secure Network Analytics

Internal Alarm IDs 7.4.2

Cisco Secure Network Analytics Internal Alarm IDs

Some previously used alarms are now obsolete and no longer listed in this file.

1	Host Lock Violation (discontinued as of v7.2.0)
5	SYN Flood
6	UDP Flood
7	ICMP Flood
8	Packet Flood
9	High Volume Email
10	Mail Relay
11	Spam Source
12	Mail Rejects
13	Watch Port Active
14	New Host Active
15	High Target Index
16	High Total Traffic
17	Max Flows Initiated
18	New Flows Initiated
19	SYNs Received
20	High File Sharing Index

24	Suspect UDP Activity
25	MAC Address Violation
26	Half Open Attack
28	Touched
29	Low Traffic
30	High Traffic
31	Watch Host Active
32	High Concern Index
33	Suspect Long Flow
34	Trapped Host
35	Worm Activity
36	Worm Propagation
37	Max Flows Served
38	New Flows Served
39	Beaconing Host
40	Data Loss
41	Bot Infected Host - Attempted C&C Activity (Partial Match)
42	Bot Infected Host - Successful C&C Activity (Full Match)
43	Bot Command & Control Server (Controlled)
44	Slow Connection Flood
45	Data Exfiltration

46	Command and Control
47	Policy Violation
48	Suspect Quiet Long Flow
49	UDP Received
50	ICMP Received
51	Recon
52	Data Hoarding
53	High DDoS Target Index
54	High DDoS Source Index
55	Port Scan
56	Exploitation
57	Anomaly
58	Brute Force Login
59	Talks to Phantoms
60	High SMB Peers
61	SSH Reverse Shell
62	Fake Application Detected
63	Scanner Talking
257	Ping
258	ICMP TimeOut
259	TimeOut UDP

260	TimeOut TCP
261	Reset UDP
262	Reset TCP
263	Bad Flag All
264	Bad Flag SYN FYN
265	Bad Flag Reserved (Sflow Only)
266	Bad Flag RST
267	Bad Flag ACK
268	Bad Flag URG
269	Bad Flag No Flag
271	Stealth Scan UDP
272	Stealth Scan TCP
273	SRC=DES
276	Addr Scan TCP
277	Ping Scan
278	Ping Oversized Packet
281	Frag Pkt Too Short
282	Frag Pkt Too Long
283	Frag Different Sizes
286	Addr Scan UDP
289	ICMP Net Unreachable

290	ICMP Host Unreachable
291	ICMP Protocol Unreachable
292	ICMP Port Unreachable
293	ICMP Frag Needed
294	ICMP SRC Route Failed
295	ICMP Dest Network Unknown
296	ICMP Dest Host Unknown
297	ICMP Src Host isolated
298	ICMP Dest Net Admin
299	ICMP Dst Host Admin
300	ICMP Net Unreachable TOS
301	ICMP Host Unreachable TOS
302	ICMP Comm Admin
303	ICMP Host Precedence
304	ICMP Precedence Cutoff
310	Flow Denied
315	Suspect Data Hoarding
316	Target Data Hoarding
317	Connection From TOR Attempted
318	Connection From TOR Successful
319	Inside TOR Exit Detected

513	Connection To TOR Attempted
514	Connection To TOR Successful
515	Inside TOR Entry Detected
516	Connection To Bogon Address Successful
517	Connection From Bogon Address Successful
518	Connection To Bogon Address Attempted
519	Connection From Bogon Address Attempted
4010	Flow Collector Flow Data Lost
4020	Interface Utilization Exceeded Inbound
4030	Interface Utilization Exceeded Outbound
4040	Flow Collector Longest Export Exceeded
5010	FlowSensor Virtual Edition Configuration Error
5011	FlowSensor Traffic Lost
5012	FlowSensor RAID Failure
5013	FlowSensor RAID Rebuilding
5998	FlowSensor Time Mismatch
5999	FlowSensor Management Channel Down
7001	Relationship High Total Traffic
7002	Relationship High Traffic
7003	Relationship Low Traffic
7004	Relationship Max Flows

7005	Relationship New Flows
7006	Relationship Round Trip Time
7007	Relationship Server Response Time
7008	Relationship TCP Retransmission Ratio
7009	Relationship SYN Flood
7010	Relationship UDP Flood
7011	Relationship ICMP Flood
9021	Flow Collector Data Deleted
9022	Flow Collector Database Unavailable
9023	Flow Collector Database Channel Down
9050	Flow Collector Exporter Count Exceeded
9051	Flow Collector FlowSensor Virtual Edition Count Exceeded
9052	Flow Collector Flow Rate Exceeded
9053	Flow Collector Interfaces Count Exceeded
9054	Flow Collector Database Updates Dropped
9100	Flow Collector RAID Failure
9102	Flow Collector RAID Rebuilding
9998	Flow Collector Performance Degraded
9999	Flow Collector Stopped
60000	Flow Collector Time Mismatch
60001	Cisco ISE Management Channel Down

60002	Flow Collector Management Channel Down
60003	SMC RAID Failure
60005	SMC RAID Rebuilding
60007	SMC Disk Space Low
60008	SMC Duplicate Primary
60012	Stealthwatch Flow License Exceeded (discontinued as of v7.2.0)
60013	License Corrupted (discontinued as of v7.2.0)
60014	Unlicensed Feature (discontinued as of v7.2.0)
60015	SLIC Channel Down
60016	UDPD Communication Down
60023	UDPD HA Down
60024	Unlicensed FPS (Flows per Second) Feature (discontinued as of v7.2.0) **Important:** This alarm is functional only in v6.9. In v6.10, it has been replaced by the Secure Network Analytics Flow Rate License Unavailable alarm (alarm ID # 60025).
60025	Stealthwatch Flow Rate License Unavailable (discontinued as of v7.2.0) **Important:** This alarm is functional beginning in v6.10. It replaces the Unlicensed FPS Feature alarm (alarm ID # 60024), which is functional only in v6.9.
60030	SMC query connection with Data Store lost
60040	SMC database ingest and maintenance connection with Data Store lost
60041	Data Node down

60042	Data Node recovering
60043	Data Store excessive timestamp skew
60044	Data Store shut down due to too many Data Nodes down
60045	Data Store recovery failure
60046	Data Node recovery error
60047	Data Node recovery lock error
60048	Data Node refresh failure
60049	Data Node down; remaining Data Node count critical
60050	Data Store reaching limit for ROS container operational files
60051	Appliance Certificate Expiration less than 90 days
60052	Appliance Certificate Expiration less than 60 days
60053	Appliance Certificate Expiration less than 30 days
60054	Appliance Certificate Expiration less than 14 days
60055	Appliance Certificate Expiration less than 3 days
60056	Appliance Certificate has expired
60080	Analytics Results Incomplete
60081	Analytics Performance Degraded
60082	Analytics Unsupported Domains
70026	UDPD RAID Failure
70027	UDPD RAID Rebuilding
70028	UDPD Stopped

70029	UDPD Degraded
600016	Identity Channel Down
600017	SMC Failover Channel Down
600018	License Term less than 90 days (discontinued as of v7.2.0)
600019	License Term less than 60 days (discontinued as of v7.2.0)
600020	License Term less than 30 days (discontinued as of v7.2.0)
600021	License Term less than 14 days (discontinued as of v7.2.0)
600022	License Term less than 3 days (discontinued as of v7.2.0)

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Change History

Document Version	Published Date	Description
1_0	February 2023	Initial version.

Copyright Information