



Log Reference Guide

Clavister® CorePlus™ Version 8.81.08

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Phone: +46-660-299200
Fax: +46-660-12250

www.clavister.com

Build: 88108
Published 2009-03-10
Copyright © 2009 Clavister AB

Log Reference Guide

Clavister® CorePlus™

Version 8.81.08

Published 2009-03-10
Build: 88108

Copyright © 2009 Clavister AB

Copyright Notice

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL CLAVISTER OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE CLAVISTER PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF CLAVISTER IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, CLAVISTER WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. CLAVISTER WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT CLAVISTER RECEIVED FROM THE END-USER FOR THE PRODUCT.

Table of Contents

Preface	23
1. Introduction	25
1.1. Log Message Structure	25
1.2. Context Parameters	27
1.3. Statistics (usage)	31
1.4. Severity levels	32
2. Log Message Reference	34
2.1. ALG	35
2.1.1. alg_session_open (ID: 00200001)	35
2.1.2. alg_session_closed (ID: 00200002)	36
2.1.3. max_line_length_exceeded (ID: 00200003)	36
2.1.4. invalid_client_http_header_received (ID: 00200100)	36
2.1.5. invalid_url_format (ID: 00200101)	37
2.1.6. unknown_client_data_received (ID: 00200105)	37
2.1.7. suspicious_data_received (ID: 00200106)	37
2.1.8. invalid_chunked_encoding (ID: 00200107)	38
2.1.9. invalid_server_http_header_received (ID: 00200108)	38
2.1.10. compressed_data_received (ID: 00200109)	38
2.1.11. max_http_sessions_reached (ID: 00200110)	39
2.1.12. failed_create_new_session (ID: 00200111)	39
2.1.13. failure_connect_http_server (ID: 00200112)	40
2.1.14. content_type_mismatch (ID: 00200113)	40
2.1.15. wcf_override_full (ID: 00200114)	40
2.1.16. content_filtering_disabled (ID: 00200115)	41
2.1.17. max_download_size_reached (ID: 00200116)	41
2.1.18. blocked_filetype (ID: 00200117)	41
2.1.19. out_of_mem (ID: 00200118)	42
2.1.20. wcf_servers_unreachable (ID: 00200119)	42
2.1.21. wcf_srv_connection_error (ID: 00200120)	42
2.1.22. wcf_server_unreachable (ID: 00200121)	43
2.1.23. wcf_connecting (ID: 00200122)	43
2.1.24. wcf_server_connected (ID: 00200123)	43
2.1.25. wcf_primary_fallback (ID: 00200124)	44
2.1.26. request_url (ID: 00200125)	44
2.1.27. request_url (ID: 00200126)	44
2.1.28. request_url (ID: 00200129)	45
2.1.29. restricted_site_notice (ID: 00200132)	45
2.1.30. url_reclassification_request (ID: 00200133)	46
2.1.31. max_smtp_sessions_reached (ID: 00200150)	46
2.1.32. maximum_email_per_minute_reached (ID: 00200151)	47
2.1.33. failed_create_new_session (ID: 00200152)	47
2.1.34. failed_connect_smtp_server (ID: 00200153)	47
2.1.35. invalid_server_response (ID: 00200155)	48
2.1.36. sender_email_id_mismatched (ID: 00200157)	48
2.1.37. sender_email_id_is_in_blacklist (ID: 00200158)	48
2.1.38. recipient_email_id_in_blacklist (ID: 00200159)	49
2.1.39. some_recipient_email_ids_are_in_blocklist (ID: 00200160)	49
2.1.40. base64_decode_failed (ID: 00200164)	49
2.1.41. base64_decode_failed (ID: 00200165)	50
2.1.42. blocked_filetype (ID: 00200166)	50
2.1.43. content_type_mismatch (ID: 00200167)	51
2.1.44. max_email_size_reached (ID: 00200170)	51
2.1.45. content_type_mismatch_mimecheck_disabled (ID: 00200171)	51
2.1.46. all_recipient_email_ids_are_in_blocklist (ID: 00200172)	52
2.1.47. out_of_memory (ID: 00200175)	52
2.1.48. invalid_end_of_mail (ID: 00200176)	53
2.1.49. dnsbl_init_error (ID: 00200177)	53

2.1.50. cmd_too_long (ID: 00200179)	53
2.1.51. cmd_empty (ID: 00200180)	54
2.1.52. failed_send_reply_code (ID: 00200181)	54
2.1.53. smtp_no_header (ID: 00200184)	54
2.1.54. unsupported_extension (ID: 00200185)	54
2.1.55. cmd_pipelined (ID: 00200186)	55
2.1.56. smtp_state_violation (ID: 00200190)	55
2.1.57. illegal_data_direction (ID: 00200202)	55
2.1.58. hybrid_data (ID: 00200206)	56
2.1.59. hybrid_data (ID: 00200209)	56
2.1.60. illegal_chars (ID: 00200210)	56
2.1.61. control_chars (ID: 00200211)	57
2.1.62. illegal_command (ID: 00200212)	57
2.1.63. illegal_command (ID: 00200213)	58
2.1.64. port_command_disabled (ID: 00200214)	58
2.1.65. illegal_command (ID: 00200215)	59
2.1.66. illegal_ip_address (ID: 00200216)	59
2.1.67. illegal_port_number (ID: 00200217)	59
2.1.68. failed_to_create_connection1 (ID: 00200218)	60
2.1.69. illegal_command (ID: 00200219)	60
2.1.70. illegal_direction1 (ID: 00200220)	61
2.1.71. illegal_direction2 (ID: 00200221)	61
2.1.72. illegal_option (ID: 00200222)	61
2.1.73. illegal_option (ID: 00200223)	62
2.1.74. unknown_option (ID: 00200224)	62
2.1.75. illegal_command (ID: 00200225)	63
2.1.76. unknown_command (ID: 00200226)	63
2.1.77. illegal_reply (ID: 00200228)	63
2.1.78. illegal_reply (ID: 00200230)	64
2.1.79. illegal_reply (ID: 00200231)	64
2.1.80. illegal_reply (ID: 00200232)	65
2.1.81. bad_port (ID: 00200233)	65
2.1.82. bad_ip (ID: 00200234)	65
2.1.83. failed_to_create_connection2 (ID: 00200235)	66
2.1.84. failed_to_create_server_data_connection (ID: 00200236)	66
2.1.85. failed_to_send_port (ID: 00200237)	67
2.1.86. failed_to_register_rawconn (ID: 00200238)	67
2.1.87. failed_to_merge_conns (ID: 00200239)	67
2.1.88. max_ftp_sessions_reached (ID: 00200241)	68
2.1.89. failed_create_new_session (ID: 00200242)	68
2.1.90. failure_connect_ftp_server (ID: 00200243)	68
2.1.91. content_type_mismatch (ID: 00200250)	69
2.1.92. failed_to_send_command (ID: 00200251)	69
2.1.93. resumed_compressed_file_transfer (ID: 00200252)	69
2.1.94. blocked_filetype (ID: 00200253)	70
2.1.95. resumed_compressed_file_transfer (ID: 00200254)	70
2.1.96. failed_to_send_response_code (ID: 00200255)	70
2.1.97. illegal_command (ID: 00200267)	71
2.1.98. unknown_state (ID: 00200300)	71
2.1.99. invalid_message (ID: 00200301)	71
2.1.100. decode_failed (ID: 00200302)	72
2.1.101. encode_failed (ID: 00200303)	72
2.1.102. encode_failed (ID: 00200304)	73
2.1.103. encode_failed (ID: 00200305)	73
2.1.104. decode_failed (ID: 00200306)	73
2.1.105. encode_failed (ID: 00200307)	74
2.1.106. max_tcp_data_connections_exceeded (ID: 00200308)	74
2.1.107. max_connections_per_call_exceeded (ID: 00200309)	75
2.1.108. ignoring_channel (ID: 00200310)	75
2.1.109. com_mode_response_message_not_translated (ID: 00200311)	75
2.1.110. max_h323_session_reached (ID: 00200312)	76
2.1.111. failed_create_new_session (ID: 00200313)	76
2.1.112. max_h323_gk_sessions_reached (ID: 00200314)	76

2.1.113. failed_create_new_session (ID: 00200315)	77
2.1.114. failure_connect_h323_server (ID: 00200316)	77
2.1.115. com_mode_command_message_not_translated (ID: 00200317)	77
2.2. ANTIVIRUS	79
2.2.1. virus_found (ID: 05800001)	79
2.2.2. virus_found (ID: 05800002)	79
2.2.3. excluded_file (ID: 05800003)	80
2.2.4. decompression_failed (ID: 05800004)	80
2.2.5. decompression_failed (ID: 05800005)	80
2.2.6. compression_ratio_violation (ID: 05800006)	81
2.2.7. compression_ratio_violation (ID: 05800007)	81
2.2.8. compression_ratio_violation (ID: 05800008)	82
2.2.9. out_of_memory (ID: 05800009)	82
2.2.10. out_of_memory (ID: 05800010)	83
2.2.11. virus_scan_failure (ID: 05800011)	83
2.2.12. virus_scan_failure (ID: 05800012)	83
2.2.13. failed_to_allocate_memory (ID: 05800014)	84
2.2.14. no_valid_license (ID: 05800015)	84
2.2.15. no_signature_database (ID: 05800016)	84
2.2.16. general_engine_error (ID: 05800017)	85
2.2.17. out_of_memory (ID: 05800018)	85
2.2.18. unknown_encoding (ID: 05800182)	85
2.2.19. unknown_encoding (ID: 05800183)	86
2.3. ARP	87
2.3.1. already_exists (ID: 00300001)	87
2.3.2. no_sender_ip (ID: 00300002)	87
2.3.3. no_sender_ip (ID: 00300003)	87
2.3.4. arp_response_broadcast (ID: 00300004)	88
2.3.5. arp_response_multicast (ID: 00300005)	88
2.3.6. mismatching_hwaddrs (ID: 00300006)	88
2.3.7. mismatching_hwaddrs_drop (ID: 00300007)	88
2.3.8. hwaddr_change (ID: 00300008)	89
2.3.9. arp_cache_size_limit_reached (ID: 00300030)	89
2.3.10. invalid_arp_sender_ip_address (ID: 00300049)	90
2.3.11. arp_access_allowed_expect (ID: 00300050)	90
2.3.12. impossible_hw_address (ID: 00300051)	90
2.3.13. arp_response_broadcast_drop (ID: 00300052)	90
2.3.14. arp_response_multicast_drop (ID: 00300053)	91
2.3.15. arp_collides_with_static (ID: 00300054)	91
2.3.16. hwaddr_change_drop (ID: 00300055)	92
2.4. AVUPDATE	93
2.4.1. av_db_update_failure (ID: 05000001)	93
2.4.2. av_database_downloaded (ID: 05000002)	93
2.4.3. av_db_already_up_to_date (ID: 05000003)	93
2.4.4. av_db_update_denied (ID: 05000004)	93
2.4.5. av_detects_invalid_system_time (ID: 05000005)	94
2.4.6. downloading_new_database (ID: 05000007)	94
2.4.7. unsynced_databases (ID: 05000008)	94
2.5. BLACKLIST	96
2.5.1. failed_to_write_list_of_blocked_hosts_to_media (ID: 04600001)	96
2.5.2. unable_to_allocate_static_entry (ID: 04600002)	96
2.5.3. unable_to_allocate_host_entry (ID: 04600003)	96
2.5.4. connection_blacklisted (ID: 04600004)	96
2.5.5. packet_blacklisted (ID: 04600005)	97
2.5.6. packet_blacklisted (ID: 04600006)	97
2.6. BUFFERS	99
2.6.1. buffers_flooded (ID: 00500001)	99
2.7. CONN	100
2.7.1. conn_open (ID: 00600001)	100
2.7.2. conn_close (ID: 00600002)	100
2.7.3. connection_table_full (ID: 00600003)	100
2.7.4. out_of_connections (ID: 00600010)	101
2.7.5. out_of_connections (ID: 00600011)	101

2.7.6. no_new_conn_for_this_packet (ID: 00600012)	101
2.7.7. no_new_conn_for_this_packet (ID: 00600013)	102
2.7.8. no_return_route (ID: 00600014)	102
2.7.9. reverse_connect_attempt (ID: 00600015)	102
2.7.10. port_0_illegal (ID: 00600020)	103
2.7.11. udp_src_port_0_illegal (ID: 00600021)	103
2.7.12. udp_src_port_0_forwarded (ID: 00600022)	103
2.7.13. conn_usage (ID: 00600023)	104
2.7.14. active_data (ID: 00600100)	104
2.7.15. passive_data (ID: 00600101)	104
2.7.16. active_data (ID: 00600102)	105
2.7.17. passive_data (ID: 00600103)	105
2.8. DEVICEMONITOR	106
2.8.1. value_above_high_threshold (ID: 054xxxxx)	106
2.8.2. value_below_low_threshold (ID: 054xxxxx)	106
2.8.3. value_below_high_threshold (ID: 054xxxxx)	106
2.8.4. value_above_low_threshold (ID: 054xxxxx)	107
2.9. DHCP	108
2.9.1. offered_ip_occupied (ID: 00700001)	108
2.9.2. lease_changed (ID: 00700002)	108
2.9.3. lease_acquired (ID: 00700003)	108
2.9.4. renewed_lease (ID: 00700004)	109
2.9.5. lease_expired (ID: 00700005)	109
2.9.6. invalid_lease_time (ID: 00700007)	109
2.9.7. invalid_server_id (ID: 00700008)	110
2.9.8. invalid_netmask (ID: 00700009)	110
2.9.9. invalid_broadcast (ID: 00700010)	110
2.9.10. invalid_offered_ip (ID: 00700011)	111
2.9.11. invalid_gateway (ID: 00700012)	111
2.9.12. offered_broadcast_equals_gateway (ID: 00700013)	111
2.9.13. ip_collision (ID: 00700014)	112
2.9.14. route_collision (ID: 00700015)	112
2.10. DHCPRELAY	114
2.10.1. unable_to_save_dhcp_relay_list (ID: 00800001)	114
2.10.2. dhcp_relay_list_saved (ID: 00800002)	114
2.10.3. dhcp_pkt_too_small (ID: 00800003)	114
2.10.4. incorrect_bootp_dhcp_cookie (ID: 00800004)	114
2.10.5. maximum_ppm_for_relayer_reached (ID: 00800005)	115
2.10.6. relayer_resuming (ID: 00800006)	115
2.10.7. hop_limit_exceeded (ID: 00800007)	115
2.10.8. client_release (ID: 00800008)	116
2.10.9. got_reply_without_transaction_state (ID: 00800009)	116
2.10.10. maximum_dhcp_client_relay_routes_reached (ID: 00800010)	116
2.10.11. unable_to_add_relay_route_since_out_of_memory (ID: 00800011)	117
2.10.12. ignored_relay_request (ID: 00800012)	117
2.10.13. no_message_type (ID: 00800013)	117
2.10.14. bad_inform_pkt_with_mismatching_source_ip_and_client_ip (ID: 00800014)	118
2.10.15. received_relayed_inform_packet_without_client_ip (ID: 00800015)	118
2.10.16. maximum_current_dhcp_relays_for_iface (ID: 00800016)	118
2.10.17. dhcp_server_is_unroutable (ID: 00800017)	119
2.10.18. unable_to_get_free_transaction_state (ID: 00800018)	119
2.10.19. invalid_gateway (ID: 00800019)	119
2.10.20. relayed_request (ID: 00800020)	120
2.10.21. relayed_request (ID: 00800021)	120
2.10.22. got_reply_on_a_non_security_equivalent_interface (ID: 00800022)	120
2.10.23. assigned_ip_not_allowed (ID: 00800023)	121
2.10.24. illegal_client_ip_assignment (ID: 00800024)	121
2.10.25. ambiguous_host_route (ID: 00800025)	121
2.10.26. relayed_dhcp_reply (ID: 00800026)	122
2.10.27. relayed_bootp_reply (ID: 00800027)	122
2.10.28. relayed_dhcp_reply (ID: 00800028)	123
2.10.29. relayed_bootp_reply (ID: 00800029)	123

2.11. DHCPSEVER	124
2.11.1. unable_to_send_response (ID: 00900001)	124
2.11.2. option_section_is_too_big_unable_to_reply (ID: 00900002)	124
2.11.3. unable_to_save_lease_db (ID: 00900003)	124
2.11.4. lease_db_successfully_saved (ID: 00900004)	124
2.11.5. dhcp_packet_too_small (ID: 00900005)	125
2.11.6. request_for_ip_from_non_bound_client_without_state (ID: 00900006)	125
2.11.7. request_for_ip_from_bound_client_without_state (ID: 00900007)	125
2.11.8. request_for_ip_from_non_bound_client_without_state (ID: 00900008)	126
2.11.9. all_ip_pools_depleted (ID: 00900010)	126
2.11.10. request_with_bad_udp_checksum (ID: 00900011)	126
2.11.11. lease_timeout (ID: 00900012)	127
2.11.12. lease_timeout (ID: 00900013)	127
2.11.13. pool_depleted (ID: 00900014)	127
2.11.14. sending_offer (ID: 00900015)	128
2.11.15. pool_depleted (ID: 00900016)	128
2.11.16. request_for_non_offered_ip (ID: 00900017)	128
2.11.17. request_for_non_bound_ip (ID: 00900018)	129
2.11.18. client_bound (ID: 00900019)	129
2.11.19. client_renewed (ID: 00900020)	129
2.11.20. got_inform_request (ID: 00900021)	130
2.11.21. decline_for_ip_on_wrong_iface (ID: 00900022)	130
2.11.22. decline_for_non_offered_ip (ID: 00900023)	130
2.11.23. declined_by_client (ID: 00900024)	131
2.11.24. request_for_ip_from_bound_client_without_state (ID: 00900025)	131
2.11.25. release_for_ip_on_wrong_iface (ID: 00900026)	132
2.11.26. released_by_client (ID: 00900027)	132
2.12. DYNROUTING	133
2.12.1. failed_to_export_route_to_ospf_process_failed_to_alloc (ID: 01100001)	133
2.12.2. route_exported_to_ospf_as (ID: 01100002)	133
2.12.3. route_unexported_from_ospf_as (ID: 01100003)	133
2.12.4. failed_to_add_route_unable_to_alloc (ID: 01100004)	134
2.12.5. route_added (ID: 01100005)	134
2.12.6. route_removed (ID: 01100006)	134
2.13. FRAG	136
2.13.1. individual_frag_timeout (ID: 02000001)	136
2.13.2. fragact_contains_frags (ID: 02000002)	136
2.13.3. fail_suspect_out_of_resources (ID: 02000003)	136
2.13.4. fail_out_of_resources (ID: 02000004)	137
2.13.5. fail_suspect_timeout (ID: 02000005)	137
2.13.6. fail_timeout (ID: 02000006)	138
2.13.7. disallowed_suspect (ID: 02000007)	138
2.13.8. drop_frags_of_disallowed_packet (ID: 02000008)	138
2.13.9. drop_frags_of_illegal_packet (ID: 02000009)	139
2.13.10. drop_extraneous_frags_of_completed_packet (ID: 02000010)	139
2.13.11. learn_state (ID: 02000011)	140
2.13.12. drop_duplicate_frag_suspect_packet (ID: 02000012)	140
2.13.13. drop_duplicate_frag (ID: 02000013)	140
2.13.14. frag_offset_plus_length_not_in_range (ID: 02000014)	141
2.13.15. no_available_fragacts (ID: 02000015)	141
2.13.16. bad_ipdatalen (ID: 02000016)	142
2.13.17. bad_ipdatalen (ID: 02000017)	142
2.13.18. overlapping_frag (ID: 02000018)	142
2.13.19. bad_offs (ID: 02000019)	143
2.13.20. duplicate_frag_with_different_length (ID: 02000020)	143
2.13.21. duplicate_frag_with_different_data (ID: 02000021)	143
2.13.22. partial_overlap (ID: 02000022)	143
2.13.23. drop_frag_disallowed_suspect_packet (ID: 02000023)	144
2.13.24. drop_frag_disallowed_packet (ID: 02000024)	144
2.13.25. already_completed (ID: 02000025)	144
2.13.26. drop_frag_failed_suspect_packet (ID: 02000026)	145
2.13.27. drop_frag_failed_packet (ID: 02000027)	145

2.13.28.	drop_frag_illegal_packet (ID: 02000028)	145
2.13.29.	fragments_available_freeing (ID: 02000100)	146
2.14.	GRE	147
2.14.1.	failed_to_setup_gre_tunnel (ID: 02200001)	147
2.14.2.	gre_bad_flags (ID: 02200002)	147
2.14.3.	gre_bad_version (ID: 02200003)	147
2.14.4.	gre_checksum_error (ID: 02200004)	147
2.14.5.	gre_length_error (ID: 02200005)	148
2.14.6.	gre_send_routing_loop_detected (ID: 02200006)	148
2.14.7.	unmatched_session_key (ID: 02200007)	148
2.14.8.	gre_routing_flag_set (ID: 02200008)	149
2.15.	HA	150
2.15.1.	peer_gone (ID: 01200001)	150
2.15.2.	peer_gone (ID: 01200002)	150
2.15.3.	conflict_both_peers_active (ID: 01200003)	150
2.15.4.	peer_has_higher_local_load (ID: 01200004)	150
2.15.5.	peer_has_lower_local_load (ID: 01200005)	151
2.15.6.	peer_has_more_connections (ID: 01200006)	151
2.15.7.	peer_has_fewer_connections (ID: 01200007)	151
2.15.8.	conflict_both_peers_inactive (ID: 01200008)	151
2.15.9.	peer_has_more_connections (ID: 01200009)	152
2.15.10.	peer_has_fewer_connections (ID: 01200010)	152
2.15.11.	peer_alive (ID: 01200011)	152
2.15.12.	heartbeat_from_unknown (ID: 01200043)	153
2.15.13.	should_have_arrived_on_sync_iface (ID: 01200044)	153
2.15.14.	activate_failed (ID: 01200050)	153
2.15.15.	merge_failed (ID: 01200051)	153
2.15.16.	ha_commit_error (ID: 01200052)	154
2.15.17.	ha_write_failed (ID: 01200053)	154
2.15.18.	ha_commit_unknown_error (ID: 01200054)	154
2.15.19.	resync_conns_to_peer (ID: 01200100)	155
2.15.20.	hasync_connection_established (ID: 01200200)	155
2.15.21.	hasync_connection_disconnected_lifetime_expired (ID: 01200201)	155
2.15.22.	hasync_connection_failed_timeout (ID: 01200202)	155
2.15.23.	resync_conns_to_peer_complete (ID: 01200300)	156
2.15.24.	disallowed_on_sync_iface (ID: 01200400)	156
2.15.25.	sync_packet_on_nonsync_iface (ID: 01200410)	156
2.15.26.	ttl_too_low (ID: 01200411)	157
2.15.27.	heartbeat_from_myself (ID: 01200412)	157
2.15.28.	config_sync_failure (ID: 01200500)	157
2.15.29.	action=deactivate reason=requested (ID: 01200616)	158
2.15.30.	action=activate reason=requested (ID: 01200617)	158
2.15.31.	action=going_online (ID: 01200618)	158
2.16.	HWM	159
2.16.1.	temperature_alarm (ID: 04000011)	159
2.16.2.	temperature_normal (ID: 04000012)	159
2.16.3.	voltage_alarm (ID: 04000021)	159
2.16.4.	voltage_normal (ID: 04000022)	160
2.16.5.	fanrpm_alarm (ID: 04000031)	160
2.16.6.	fanrpm_normal (ID: 04000032)	161
2.16.7.	gpio_alarm (ID: 04000041)	161
2.16.8.	gpio_normal (ID: 04000042)	161
2.16.9.	free_memory_warning_level (ID: 04000101)	162
2.16.10.	free_memory_warning_level (ID: 04000102)	162
2.16.11.	free_memory_normal_level (ID: 04000103)	163
2.17.	IDP	164
2.17.1.	scan_detected (ID: 01300001)	164
2.17.2.	idp_notice (ID: 01300002)	164
2.17.3.	intrusion_detected (ID: 01300003)	165
2.17.4.	virus_detected (ID: 01300004)	165
2.17.5.	scan_detected (ID: 01300005)	166
2.17.6.	idp_notice (ID: 01300006)	166
2.17.7.	intrusion_detected (ID: 01300007)	167

2.17.8.	virus_detected (ID: 01300008)	167
2.17.9.	invalid_url_format (ID: 01300009)	168
2.17.10.	invalid_url_format (ID: 01300010)	168
2.17.11.	idp_evasion (ID: 01300011)	168
2.17.12.	idp_evasion (ID: 01300012)	169
2.17.13.	idp_outofmem (ID: 01300013)	169
2.17.14.	idp_outofmem (ID: 01300014)	170
2.17.15.	idp_failscan (ID: 01300015)	170
2.17.16.	idp_failscan (ID: 01300016)	171
2.18.	IDPUPDATE	172
2.18.1.	idp_db_update_failure (ID: 01400001)	172
2.18.2.	idp_database_downloaded (ID: 01400002)	172
2.18.3.	idp_db_already_up_to_date (ID: 01400003)	172
2.18.4.	idp_db_update_denied (ID: 01400004)	172
2.18.5.	idp_detects_invalid_system_time (ID: 01400005)	173
2.18.6.	downloading_new_database (ID: 01400007)	173
2.18.7.	unsynced_databases (ID: 01400009)	173
2.19.	IFACEMON	175
2.19.1.	ifacemon_status_bad_rereport (ID: 03900001)	175
2.19.2.	ifacemon_status_bad (ID: 03900003)	175
2.19.3.	ifacemon_status_bad (ID: 03900004)	175
2.20.	IGMP	177
2.20.1.	querier_election_won (ID: 04200001)	177
2.20.2.	querier_election_lost (ID: 04200002)	177
2.20.3.	invalid_dest_ip_address (ID: 04200003)	177
2.20.4.	invalid_destination_ethernet_address (ID: 04200004)	178
2.20.5.	failed_restarting_igmp_conn (ID: 04200006)	178
2.20.6.	invalid_size_query_packet (ID: 04200007)	178
2.20.7.	invalid_query_group_address (ID: 04200008)	179
2.20.8.	igmp_query_dropped (ID: 04200009)	179
2.20.9.	igmp_query_received (ID: 04200010)	179
2.20.10.	bad_src (ID: 04200011)	180
2.20.11.	igmp_report_received (ID: 04200012)	180
2.20.12.	packet_includes_aux_data (ID: 04200013)	181
2.20.13.	invalid_size_report_packet (ID: 04200014)	181
2.20.14.	bad_grp (ID: 04200015)	182
2.20.15.	invalid_report_grp_record (ID: 04200016)	182
2.20.16.	igmp_report_dropped (ID: 04200017)	182
2.20.17.	igmp_ruleset_rejects_report (ID: 04200018)	183
2.20.18.	bad_inet (ID: 04200019)	183
2.20.19.	max_global_requests_per_second_reached (ID: 04200020)	183
2.20.20.	max_if_requests_per_second_reached (ID: 04200021)	184
2.20.21.	disallowed_igmp_version (ID: 04200022)	184
2.20.22.	received_unknown_igmp_type (ID: 04200023)	184
2.20.23.	older_querier_present (ID: 04200024)	185
2.20.24.	older_querier_gone (ID: 04200025)	185
2.21.	IPPOOL	186
2.21.1.	no_offer_received (ID: 01900001)	186
2.21.2.	no_valid_dhcp_offer_received (ID: 01900002)	186
2.21.3.	too_many_dhcp_offers_received (ID: 01900003)	186
2.21.4.	lease_disallowed_by_lease_filter (ID: 01900004)	186
2.21.5.	lease_disallowed_by_server_filter (ID: 01900005)	187
2.21.6.	lease_have_bad_dhcp_server (ID: 01900006)	187
2.21.7.	lease_have_bad_netmask (ID: 01900007)	187
2.21.8.	lease_have_bad_offered_broadcast (ID: 01900008)	188
2.21.9.	lease_have_bad_offered_ip (ID: 01900009)	188
2.21.10.	lease_have_bad_gateway_ip (ID: 01900010)	188
2.21.11.	lease_ip_is_already_occupied (ID: 01900011)	189
2.21.12.	lease_rejected_by_server (ID: 01900012)	189
2.21.13.	ip_offer_already_exist_in_the_pool (ID: 01900013)	189
2.21.14.	pool_reached_max_dhcp_clients (ID: 01900014)	190
2.21.15.	macrange_depleted (ID: 01900015)	190
2.21.16.	ip_fetched_pool (ID: 01900016)	190

2.21.17. ip_returned_to_pool (ID: 01900017)	191
2.22. IPSEC	192
2.22.1. fatal_ipsec_event (ID: 01800100)	192
2.22.2. warning_ipsec_event (ID: 01800101)	192
2.22.3. audit_event (ID: 01800103)	192
2.22.4. audit_flood (ID: 01800104)	193
2.22.5. ike_delete_notification (ID: 01800105)	193
2.22.6. ike_invalid_payload (ID: 01800106)	193
2.22.7. ike_invalid_proposal (ID: 01800107)	194
2.22.8. ike_retry_limit_reached (ID: 01800108)	194
2.22.9. ike_quickmode_failed (ID: 01800109)	194
2.22.10. packet_corrupt (ID: 01800110)	195
2.22.11. icv_failure (ID: 01800111)	195
2.22.12. sequence_number_failure (ID: 01800112)	195
2.22.13. sa_lookup_failure (ID: 01800113)	196
2.22.14. ip_fragment (ID: 01800114)	196
2.22.15. sequence_number_overflow (ID: 01800115)	196
2.22.16. bad_padding (ID: 01800116)	197
2.22.17. hardware_accelerator_congested (ID: 01800117)	197
2.22.18. hardware_acceleration_failure (ID: 01800118)	198
2.22.19. commit_failed (ID: 01800200)	198
2.22.20. commit_succeeded (ID: 01800201)	198
2.22.21. IPsec_successfully_started (ID: 01800202)	199
2.22.22. x509_init_failed (ID: 01800203)	199
2.22.23. pm_create_failed (ID: 01800204)	199
2.22.24. failed_to_start_ipsec (ID: 01800206)	199
2.22.25. failed_create_audit_module (ID: 01800207)	200
2.22.26. failed_to_configure_IPsec (ID: 01800210)	200
2.22.27. reconfig_IPsec (ID: 01800211)	200
2.22.28. IPsec_init_failed (ID: 01800213)	200
2.22.29. ipsec_started_successfully (ID: 01800214)	201
2.22.30. Failed_to_add_certificate (ID: 01800302)	201
2.22.31. Default_IKE_DH_groups_will_be_used (ID: 01800303)	201
2.22.32. failed_to_set_algorithm_properties (ID: 01800304)	201
2.22.33. failed_to_set_algorithm_properties (ID: 01800305)	202
2.22.34. failed_to_add_root_certificate (ID: 01800306)	202
2.22.35. dns_resolve_failed (ID: 01800308)	202
2.22.36. dns_resolve_failed (ID: 01800309)	203
2.22.37. failed_to_add_peer (ID: 01800312)	203
2.22.38. failed_to_add_rules (ID: 01800313)	203
2.22.39. failed_to_add_rules (ID: 01800314)	204
2.22.40. new_remote_gw_ip (ID: 01800315)	204
2.22.41. no_policymanager (ID: 01800316)	204
2.22.42. peer_is_dead (ID: 01800317)	205
2.22.43. failed_to_set_dpd_cb (ID: 01800318)	205
2.22.44. failed_to_add_key_provider (ID: 01800321)	205
2.22.45. failed_to_add_certificate (ID: 01800322)	206
2.22.46. failed_to_set_remote_ID (ID: 01800323)	206
2.22.47. failed_to_create_authorization (ID: 01800327)	206
2.22.48. Failed_to_set_xauth (ID: 01800328)	206
2.22.49. Failed_to_create_xauth_group (ID: 01800329)	207
2.22.50. ippool_does_not_exist (ID: 01800400)	207
2.22.51. cfgmode_ip_freed (ID: 01800402)	207
2.22.52. recieved_packet_to_disabled_IPsec (ID: 01800500)	208
2.22.53. recieved_packet_to_disabled_IPsec (ID: 01800501)	208
2.22.54. Recieved_plaintext_packet_for_disabled_IPsec_interface (ID: 01800502)	208
2.22.55. no_remote_gateway (ID: 01800503)	208
2.22.56. no_route (ID: 01800504)	209
2.22.57. ping_heartbeat_failed_in_tunnel (ID: 01800505)	209
2.22.58. ipsec_interface_disabled (ID: 01800506)	209
2.22.59. maximum_allowed_tunnels_limit_reached (ID: 01800900)	210
2.22.60. SAs_not_killed_for_remote_peer (ID: 01800901)	210

2.22.61. trigger_non_ip_packet (ID: 01802001)	210
2.22.62. rule_not_active (ID: 01802002)	210
2.22.63. malformed_packet (ID: 01802003)	211
2.22.64. max_ipsec_sa_negotiations_reached (ID: 01802004)	211
2.22.65. max_number_of_tunnels_reached (ID: 01802011)	211
2.22.66. ike_sa_failed (ID: 01802022)	212
2.22.67. ike_sa_negotiation_completed (ID: 01802024)	212
2.22.68. ike_sa_negotiation_failed (ID: 01802030)	212
2.22.69. ike_sa_negotiation_failed (ID: 01802031)	213
2.22.70. ipsec_sa_negotiation_completed (ID: 01802040)	213
2.22.71. ipsec_sa_informal (ID: 01802041)	213
2.22.72. ipsec_sa_informal (ID: 01802043)	214
2.22.73. ipsec_sa_informal (ID: 01802044)	214
2.22.74. ipsec_sa_lifetime (ID: 01802045)	214
2.22.75. ipsec_sa_lifetime (ID: 01802046)	215
2.22.76. ipsec_sa_lifetime (ID: 01802047)	215
2.22.77. ipsec_sa_lifetime (ID: 01802048)	215
2.22.78. ipsec_sa_informal (ID: 01802058)	215
2.22.79. ipsec_invalid_protocol (ID: 01802059)	216
2.22.80. ipsec_sa_negotiation_aborted (ID: 01802060)	216
2.22.81. create_rules_failed (ID: 01802080)	216
2.22.82. create_rules_failed (ID: 01802081)	217
2.22.83. no_authentication_method_specified (ID: 01802100)	217
2.22.84. no_key_method_configured_for_tunnel (ID: 01802102)	217
2.22.85. invalid_configuration_of_force_open (ID: 01802104)	217
2.22.86. invalid_rule_setting (ID: 01802105)	218
2.22.87. invalid_rule_setting (ID: 01802106)	218
2.22.88. invalid_rule_setting (ID: 01802107)	218
2.22.89. invalid_rule_setting (ID: 01802108)	219
2.22.90. invalid_rule_setting (ID: 01802109)	219
2.22.91. max_number_of_policy_rules_reached (ID: 01802110)	219
2.22.92. suspicious_outbound_rule (ID: 01802114)	219
2.22.93. no_algorithms_configured_for_tunnel (ID: 01802200)	220
2.22.94. no_encryption_algorithm_configured_for_tunnel (ID: 01802201)	220
2.22.95. no_authentication_algorithm_specified (ID: 01802203)	220
2.22.96. AH_not_supported (ID: 01802204)	221
2.22.97. invalid_tunnel_configuration (ID: 01802208)	221
2.22.98. invalid_tunnel_configuration (ID: 01802209)	221
2.22.99. invalid_tunnel_configuration (ID: 01802210)	221
2.22.100. out_of_memory_for_tunnel (ID: 01802211)	222
2.22.101. invalid_key_size (ID: 01802214)	222
2.22.102. invalid_key_size (ID: 01802215)	222
2.22.103. invalid_key_size (ID: 01802216)	223
2.22.104. invalid_key_size (ID: 01802217)	223
2.22.105. invalid_cipher_keysize (ID: 01802218)	223
2.22.106. invalid_key_size (ID: 01802219)	223
2.22.107. invalid_cipher_keysize (ID: 01802220)	224
2.22.108. malformed_tunnel_id_configured (ID: 01802225)	224
2.22.109. malformed_psk_configured (ID: 01802229)	224
2.22.110. rule_selection_failed (ID: 01802300)	225
2.22.111. max_phase1_sa_reached (ID: 01802400)	225
2.22.112. max_phase1_negotiations_reached (ID: 01802402)	225
2.22.113. max_active_quickmode_negotiation_reached (ID: 01802403)	225
2.22.114. could_not_decode_certificate (ID: 01802600)	226
2.22.115. could_not_convert_certificate (ID: 01802601)	226
2.22.116. could_not_get_subject_name_from_ca_cert (ID: 01802602)	226
2.22.117. could_not_set_cert_to_non_CRL_issuer (ID: 01802603)	226
2.22.118. could_not_force_cert_to_be_trusted (ID: 01802604)	227
2.22.119. could_not_trusted_set_for_cert (ID: 01802605)	227
2.22.120. could_not_insert_cert_to_db (ID: 01802606)	227
2.22.121. could_not_decode_certificate (ID: 01802607)	228
2.22.122. could_not_load_certificate (ID: 01802608)	228
2.22.123. could_not_insert_cert_to_db (ID: 01802609)	228

2.22.124. could_not_decode_crl (ID: 01802610)	228
2.22.125. ike_sa_negotiation_completed (ID: 01802703)	229
2.22.126. ike_sa_negotiation_completed (ID: 01802704)	229
2.22.127. Certificate_contains_bad_IP_address (ID: 01802705)	229
2.22.128. dn_name_as_subject_alt_name (ID: 01802706)	230
2.22.129. could_not_decode_certificate (ID: 01802707)	230
2.22.130. ike_sa_destroyed (ID: 01802708)	230
2.22.131. cfgmode_exchange_event (ID: 01802709)	230
2.22.132. remote_access_address (ID: 01802710)	231
2.22.133. remote_access_dns (ID: 01802711)	231
2.22.134. remote_access_wins (ID: 01802712)	231
2.22.135. remote_access_dhcp (ID: 01802713)	232
2.22.136. remote_access_subnets (ID: 01802714)	232
2.22.137. event_on_ike_sa (ID: 01802715)	232
2.22.138. ipsec_sa_selection_failed (ID: 01802717)	233
2.22.139. certificate_search_failed (ID: 01802718)	233
2.22.140. ipsec_sa_event (ID: 01802730)	233
2.22.141. ipsec_sa_event (ID: 01802731)	234
2.22.142. ipsec_sa_destroyed (ID: 01802732)	234
2.22.143. (ID: 01802735)	234
2.22.144. (ID: 01802736)	235
2.22.145. outofmem_create_engine (ID: 01802901)	235
2.22.146. init_rulelookup_failed (ID: 01802903)	235
2.22.147. init_rule_lookup_failed (ID: 01802904)	235
2.22.148. init_rule_lookup_failed (ID: 01802905)	236
2.22.149. init_mutexes_failed (ID: 01802906)	236
2.22.150. init_interface_table_failed (ID: 01802907)	236
2.22.151. init_flow_id_table_failed (ID: 01802908)	236
2.22.152. init_flow_table_failed (ID: 01802909)	237
2.22.153. init_next_hop_table_failed (ID: 01802910)	237
2.22.154. init_transform_table_failed (ID: 01802911)	237
2.22.155. init_peer_hash_failed (ID: 01802912)	237
2.22.156. init_peer_id_hash_failed (ID: 01802913)	238
2.22.157. init_rule_table_failed (ID: 01802914)	238
2.22.158. init_inbound_spi_hash_failed (ID: 01802915)	238
2.22.159. init_transform_context_hash_failed (ID: 01802916)	238
2.22.160. init_packet_context_cache_failed (ID: 01802917)	239
2.22.161. init_transform_context_table_failed (ID: 01802918)	239
2.22.162. init_nat_table_failed (ID: 01802919)	239
2.22.163. init_frag_table_failed (ID: 01802920)	240
2.22.164. init_engine_tables_failed (ID: 01802921)	240
2.22.165. init_interceptor_failed (ID: 01802922)	240
2.22.166. malformed_ike_sa_proposal (ID: 01803000)	240
2.22.167. failed_to_select_policy_rule (ID: 01803001)	241
2.22.168. failed_to_select_ike_sa (ID: 01803002)	241
2.22.169. ike_phase1_notification (ID: 01803003)	241
2.22.170. ipsec_sa_failed (ID: 01803020)	241
2.22.171. ipsec_sa_statistics (ID: 01803021)	242
2.22.172. config_mode_exchange_event (ID: 01803022)	242
2.22.173. config_mode_exchange_event (ID: 01803023)	242
2.22.174. xauth_exchange_done (ID: 01803024)	243
2.22.175. config_mode_exchange_event (ID: 01803025)	243
2.22.176. config_mode_exchange_event (ID: 01803026)	243
2.22.177. rejecting_ipsec_sa_delete (ID: 01803027)	244
2.22.178. rejecting_ipsec_sa_delete (ID: 01803028)	244
2.22.179. ike_phase2_notification (ID: 01803029)	244
2.22.180. ike_qm_notification (ID: 01803030)	245
2.22.181. failed_to_verify_peer_identity (ID: 01803040)	245
2.22.182. malformed_ipsec_sa_proposal (ID: 01803050)	245
2.22.183. malformed_ipsec_esp_proposal (ID: 01803051)	246
2.22.184. malformed_ipsec_ah_proposal (ID: 01803052)	246
2.22.185. failed_to_select_ipsec_proposal (ID: 01803053)	246
2.22.186. failed_to_select_ipsec_sa (ID: 01803054)	246

2.22.187. ike_responder_mode_not_available (ID: 01803101)	247
2.22.188. audit_event (ID: 01803200)	247
2.22.189. failed_to_find_userauthobject_for_ipsec_sa (ID: 01803302)	247
2.23. IP_ERROR	249
2.23.1. too_small_packet (ID: 01500001)	249
2.23.2. disallowed_ip_ver (ID: 01500002)	249
2.23.3. invalid_ip_length (ID: 01500003)	249
2.23.4. invalid_ip_length (ID: 01500004)	250
2.23.5. invalid_ip_checksum (ID: 01500005)	250
2.24. IP_FLAG	251
2.24.1. ttl_low (ID: 01600001)	251
2.24.2. ip_rsv_flag_set (ID: 01600002)	251
2.24.3. ip_rsv_flag_set (ID: 01600003)	251
2.25. IP_OPT	253
2.25.1. source_route (ID: 01700001)	253
2.25.2. timestamp (ID: 01700002)	253
2.25.3. router_alert (ID: 01700003)	253
2.25.4. ipopt_present (ID: 01700004)	254
2.25.5. ipoptlen_too_small (ID: 01700010)	254
2.25.6. ipoptlen_invalid (ID: 01700011)	254
2.25.7. multiple_ip_option_routes (ID: 01700012)	255
2.25.8. bad_length (ID: 01700013)	255
2.25.9. bad_route_pointer (ID: 01700014)	255
2.25.10. source_route_disallowed (ID: 01700015)	256
2.25.11. multiple_ip_option_timestamps (ID: 01700016)	256
2.25.12. bad_timestamp_len (ID: 01700017)	256
2.25.13. bad_timestamp_pointer (ID: 01700018)	257
2.25.14. bad_timestamp_pointer (ID: 01700019)	257
2.25.15. timestamp_disallowed (ID: 01700020)	257
2.25.16. router_alert_bad_len (ID: 01700021)	258
2.25.17. router_alert_disallowed (ID: 01700022)	258
2.25.18. ipopt_present_disallowed (ID: 01700023)	258
2.26. IP_PROTO	260
2.26.1. multicast_ethernet_ip_address_mismatch (ID: 07000011)	260
2.26.2. invalid_ip4_header_length (ID: 07000012)	260
2.26.3. ttl_zero (ID: 07000013)	260
2.26.4. ttl_low (ID: 07000014)	261
2.26.5. ip_rsv_flag_set (ID: 07000015)	261
2.26.6. oversize_tcp (ID: 07000018)	261
2.26.7. invalid_tcp_header (ID: 07000019)	262
2.26.8. oversize_udp (ID: 07000021)	262
2.26.9. invalid_udp_header (ID: 07000022)	262
2.26.10. oversize_icmp (ID: 07000023)	263
2.26.11. invalid_icmp_header (ID: 07000024)	263
2.26.12. multicast_ethernet_ip_address_mismatch (ID: 07000033)	264
2.26.13. oversize_gre (ID: 07000050)	264
2.26.14. oversize_esp (ID: 07000051)	264
2.26.15. oversize_ah (ID: 07000052)	265
2.26.16. oversize_skip (ID: 07000053)	265
2.26.17. oversize_ospf (ID: 07000054)	265
2.26.18. oversize_ipip (ID: 07000055)	266
2.26.19. oversize_ipcomp (ID: 07000056)	266
2.26.20. oversize_l2tp (ID: 07000057)	266
2.26.21. oversize_ip (ID: 07000058)	267
2.26.22. fragmented_icmp (ID: 07000070)	267
2.26.23. invalid_icmp_data_too_small (ID: 07000071)	267
2.26.24. invalid_icmp_data_ip_ver (ID: 07000072)	268
2.26.25. invalid_icmp_data_too_small (ID: 07000073)	268
2.26.26. invalid_icmp_data_invalid_ip_length (ID: 07000074)	269
2.26.27. invalid_icmp_data_invalid_paramprob (ID: 07000075)	269
2.27. L2TP	270
2.27.1. l2tpclient_resolve_successful (ID: 02800001)	270
2.27.2. l2tpclient_resolve_failed (ID: 02800002)	270

2.27.3. l2tpclient_init (ID: 02800003)	270
2.27.4. l2tp_connection_disallowed (ID: 02800004)	271
2.27.5. unknown_l2tp_auth_source (ID: 02800005)	271
2.27.6. only_routes_set_up_by_server_iface_allowed (ID: 02800006)	271
2.27.7. l2tp_session_closed (ID: 02800007)	272
2.27.8. l2tp_tunnel_closed (ID: 02800008)	272
2.27.9. session_closed (ID: 02800009)	272
2.27.10. l2tp_session_request (ID: 02800010)	273
2.27.11. l2tp_session_up (ID: 02800011)	273
2.27.12. l2tp_no_userauth_rule_found (ID: 02800014)	273
2.27.13. l2tp_session_request (ID: 02800015)	274
2.27.14. l2tp_session_up (ID: 02800016)	274
2.27.15. failure_init_radius_accounting (ID: 02800017)	274
2.27.16. l2tpclient_tunnel_up (ID: 02800018)	275
2.27.17. malformed_packet (ID: 02800019)	275
2.27.18. waiting_for_ip_to_listen_on (ID: 02800050)	275
2.28. LICUPDATE	276
2.28.1. license_update_failure (ID: 05500001)	276
2.28.2. license_downloaded (ID: 05500002)	276
2.28.3. license_already_up_to_date (ID: 05500003)	276
2.29. NETCON	277
2.29.1. init_complete (ID: 02300001)	277
2.29.2. netcon_connect_reject_shutdown_running (ID: 02300002)	277
2.29.3. disallowed_netcon_ping (ID: 02300003)	277
2.29.4. netcon_sessionmanager_error (ID: 02300101)	278
2.29.5. cert_upload_aborted (ID: 02300200)	278
2.29.6. cert_upload_failed (ID: 02300201)	278
2.29.7. cert_upload_begin (ID: 02300202)	278
2.29.8. upload_fail_disk_out_of_space (ID: 02300250)	279
2.29.9. upload_fail_disk_cannot_remove (ID: 02300251)	279
2.29.10. disk_out_of_space (ID: 02300252)	280
2.29.11. disk_write_error (ID: 02300300)	280
2.29.12. upload_complete (ID: 02300350)	280
2.29.13. concurrent_processing_limit_reached (ID: 02300400)	281
2.29.14. netcon_init_fail_listen_socket_fail (ID: 02300500)	281
2.29.15. netcon_init_fail_security_file_corrupt (ID: 02300501)	281
2.29.16. disallowed_netcon_connect (ID: 02300502)	282
2.29.17. netcon_connect (ID: 02300503)	282
2.29.18. netcon_disconnect (ID: 02300504)	282
2.29.19. disk_cannot_write (ID: 02300505)	283
2.29.20. keychange_successful (ID: 02300506)	283
2.29.21. keychange_fail (ID: 02300507)	283
2.29.22. disk_cannot_read_old_keys (ID: 02300508)	284
2.29.23. download_fail (ID: 02300509)	284
2.29.24. concurrent_netcon_processing (ID: 02300510)	284
2.29.25. disk_cannot_write (ID: 02300511)	285
2.29.26. upload_begin (ID: 02300512)	285
2.29.27. upload_begin (ID: 02300513)	285
2.29.28. disk_cannot_read_download_fail (ID: 02300514)	286
2.29.29. download_begin (ID: 02300515)	286
2.29.30. upload_abort (ID: 02300516)	286
2.29.31. upload_fail (ID: 02300517)	287
2.29.32. download_complete (ID: 02300518)	287
2.30. OSPF	288
2.30.1. internal_error (ID: 02400001)	288
2.30.2. internal_error (ID: 02400002)	288
2.30.3. unable_to_map_ptp_neighbor (ID: 02400003)	288
2.30.4. bad_packet_len (ID: 02400004)	289
2.30.5. bad_ospf_version (ID: 02400005)	289
2.30.6. sender_not_in_iface_range (ID: 02400006)	289
2.30.7. area_mismatch (ID: 02400007)	290
2.30.8. hello_netmask_mismatch (ID: 02400008)	290
2.30.9. hello_interval_mismatch (ID: 02400009)	290

2.30.10. hello_rtr_dead_mismatch (ID: 02400010)	291
2.30.11. hello_e_flag_mismatch (ID: 02400011)	291
2.30.12. hello_n_flag_mismatch (ID: 02400012)	292
2.30.13. both_np_and_e_flag_set (ID: 02400013)	292
2.30.14. unknown_lsa_type (ID: 02400014)	292
2.30.15. auth_mismatch (ID: 02400050)	293
2.30.16. bad_auth_password (ID: 02400051)	293
2.30.17. bad_auth_crypto_key_id (ID: 02400052)	293
2.30.18. bad_auth_crypto_seq_number (ID: 02400053)	294
2.30.19. bad_auth_crypto_digest (ID: 02400054)	294
2.30.20. checksum_mismatch (ID: 02400055)	294
2.30.21. dd_mtu_exceeds_interface_mtu (ID: 02400100)	295
2.30.22. m_ms_mismatch (ID: 02400101)	295
2.30.23. i_flag_misuse (ID: 02400102)	295
2.30.24. opt_change (ID: 02400103)	296
2.30.25. bad_seq_num (ID: 02400104)	296
2.30.26. non_dup_dd (ID: 02400105)	296
2.30.27. as_ext_on_stub (ID: 02400106)	297
2.30.28. unknown_lsa (ID: 02400107)	297
2.30.29. bad_lsa_sequencenumber (ID: 02400108)	297
2.30.30. bad_lsa_maxage (ID: 02400109)	298
2.30.31. lsa_checksum_mismatch (ID: 02400150)	298
2.30.32. unknown_lsa_type (ID: 02400151)	298
2.30.33. bad_lsa_sequencenumber (ID: 02400152)	299
2.30.34. bad_lsa_maxage (ID: 02400153)	299
2.30.35. received_as_ext_on_stub (ID: 02400154)	299
2.30.36. received_selforg_for_unknown_lsa_type (ID: 02400155)	300
2.30.37. db_copy_more_recent_than_received (ID: 02400156)	300
2.30.38. got_ack_mismatched_lsa (ID: 02400157)	300
2.30.39. upd_packet_lsa_size_mismatch (ID: 02400158)	301
2.30.40. req_packet_lsa_size_mismatch (ID: 02400159)	301
2.30.41. ack_packet_lsa_size_mismatch (ID: 02400160)	301
2.30.42. failed_to_create_replacement_lsa (ID: 02400161)	302
2.30.43. unable_to_send_ack (ID: 02400162)	302
2.30.44. unknown_neighbor (ID: 02400200)	302
2.30.45. too_many_neighbors (ID: 02400201)	303
2.30.46. neighbor_died (ID: 02400202)	303
2.30.47. unable_to_find_transport_area (ID: 02400300)	303
2.30.48. internal_error_unable_to_map_identifier (ID: 02400301)	304
2.30.49. lsa_size_too_big (ID: 02400302)	304
2.30.50. memory_usage_exceeded_70_percent_of_max_allowed (ID: 02400303)	304
2.30.51. memory_usage_exceeded_90_percent_of_max_allowed (ID: 02400304)	305
2.30.52. as_disabled_due_to_mem_alloc_fail (ID: 02400305)	305
2.30.53. internal_lsa_chksum_error (ID: 02400306)	305
2.30.54. unable_to_find_iface_to_stub_net (ID: 02400400)	306
2.30.55. internal_error_unable_to_find_lnk_connecting_to_lsa (ID: 02400401)	306
2.30.56. internal_error_unable_to_find_iface_connecting_to_lsa (ID: 02400402)	306
2.30.57. internal_error_unable_to_find_lnk_connecting_to_lsa (ID: 02400403)	307
2.30.58. internal_error_unable_to_find_iface_connecting_to_lsa (ID: 02400404)	307
2.30.59. internal_error_unable_neighbor_iface_attached_back_to_me (ID: 02400405)	307
2.30.60. bad_iface_type_mapping_rtr_to_rtr_link (ID: 02400406)	308
2.30.61. internal_error_unable_to_find_lnk_connecting_to_lsa (ID: 02400407)	308
2.30.62. memory_allocation_failure (ID: 02400500)	308
2.30.63. unable_to_send (ID: 02400501)	309
2.30.64. failed_to_add_route (ID: 02400502)	309
2.31. PPP	310
2.31.1. ip_pool_empty (ID: 02500001)	310
2.31.2. ip_address_required_but_not_received (ID: 02500002)	310

2.31.3.	primary_dns_address_required_but_not_received (ID: 02500003)	310
2.31.4.	secondary_dns_address_required_but_not_received (ID: 02500004) ...	311
2.31.5.	primary_nbns_address_required_but_not_received (ID: 02500005) ...	311
2.31.6.	secondary_nbns_address_required_but_not_received (ID: 02500006) .	311
2.31.7.	failed_to_agree_on_authentication_protocol (ID: 02500050)	312
2.31.8.	peer_refuses_to_use_authentication (ID: 02500051)	312
2.31.9.	lcp_negotiation_stalled (ID: 02500052)	312
2.31.10.	ppp_tunnel_limit_exceeded (ID: 02500100)	313
2.31.11.	authentication_failed (ID: 02500101)	313
2.31.12.	response_value_too_long (ID: 02500150)	313
2.31.13.	username_too_long (ID: 02500151)	314
2.31.14.	username_too_long (ID: 02500201)	314
2.31.15.	username_too_long (ID: 02500301)	314
2.31.16.	username_too_long (ID: 02500350)	314
2.31.17.	password_too_long (ID: 02500351)	315
2.31.18.	unsupported_auth_server (ID: 02500500)	315
2.31.19.	radius_error (ID: 02500501)	315
2.31.20.	authdb_error (ID: 02500502)	316
2.31.21.	MPPE_decrypt_fail (ID: 02500600)	316
2.32.	PPPOE	317
2.32.1.	pppoe_tunnel_up (ID: 02600001)	317
2.32.2.	pppoe_tunnel_closed (ID: 02600002)	317
2.33.	PPTP	318
2.33.1.	pptpclient_resolve_successful (ID: 02700001)	318
2.33.2.	pptpclient_resolve_failed (ID: 02700002)	318
2.33.3.	pptp_connection_disallowed (ID: 02700003)	318
2.33.4.	unknown_pptp_auth_source (ID: 02700004)	319
2.33.5.	user_disconnected (ID: 02700005)	319
2.33.6.	only_routes_set_up_by_server_iface_allowed (ID: 02700006)	319
2.33.7.	mppe_required (ID: 02700007)	320
2.33.8.	pptp_session_closed (ID: 02700008)	320
2.33.9.	pptp_session_request (ID: 02700009)	320
2.33.10.	unsupported_message (ID: 02700010)	321
2.33.11.	failure_init_radius_accounting (ID: 02700011)	321
2.33.12.	pptp_session_up (ID: 02700012)	321
2.33.13.	pptp_session_up (ID: 02700013)	322
2.33.14.	tunnel_idle_timeout (ID: 02700014)	322
2.33.15.	session_idle_timeout (ID: 02700015)	323
2.33.16.	pptpclient_start (ID: 02700017)	323
2.33.17.	pptpclient_connected (ID: 02700018)	323
2.33.18.	pptp_tunnel_up (ID: 02700019)	324
2.33.19.	ctrlconn_refused (ID: 02700020)	324
2.33.20.	pptp_tunnel_up (ID: 02700021)	324
2.33.21.	pptp_tunnel_closed (ID: 02700022)	325
2.33.22.	pptp_connection_disallowed (ID: 02700024)	325
2.33.23.	unknown_pptp_auth_source (ID: 02700025)	325
2.33.24.	pptp_no_userauth_rule_found (ID: 02700026)	326
2.33.25.	malformed_packet (ID: 02700027)	326
2.33.26.	waiting_for_ip_to_listen_on (ID: 02700050)	326
2.34.	REASSEMBLY	327
2.34.1.	ack_of_not_transmitted_data (ID: 04800002)	327
2.34.2.	invalid_tcp_checksum (ID: 04800003)	327
2.34.3.	mismatching_data_in_overlapping_tcp_segment (ID: 04800004)	327
2.34.4.	memory_allocation_failure (ID: 04800005)	328
2.34.5.	drop_due_to_buffer_starvation (ID: 04800007)	328
2.34.6.	failed_to_send_ack (ID: 04800008)	328
2.34.7.	processing_memory_limit_reached (ID: 04800009)	328
2.34.8.	maximum_connections_limit_reached (ID: 04800010)	329
2.34.9.	state_memory_allocation_failed (ID: 04800011)	329
2.35.	RFO	330
2.35.1.	has_ping (ID: 04100001)	330
2.35.2.	no_ping (ID: 04100002)	330
2.35.3.	no_ping (ID: 04100003)	330

2.35.4. unable_to_register_pingmon (ID: 04100004)	331
2.35.5. unable_to_register_pingmon (ID: 04100005)	331
2.35.6. has_arp (ID: 04100006)	331
2.35.7. no_arp (ID: 04100007)	332
2.35.8. unable_to_register_arp_monitor (ID: 04100008)	332
2.35.9. unable_to_register_arp_monitor (ID: 04100009)	332
2.35.10. no_link (ID: 04100010)	333
2.35.11. has_link (ID: 04100011)	333
2.35.12. unable_to_register_interface_monitor (ID: 04100012)	334
2.35.13. unable_to_register_interface_monitor (ID: 04100013)	334
2.35.14. hostmon_failed (ID: 04100014)	334
2.35.15. hostmon_successful (ID: 04100015)	335
2.36. RULE	336
2.36.1. ruleset_fwdfast (ID: 06000003)	336
2.36.2. ip_verified_access (ID: 06000005)	336
2.36.3. block0net (ID: 06000010)	336
2.36.4. block0net (ID: 06000011)	337
2.36.5. block127net (ID: 06000012)	337
2.36.6. block127net (ID: 06000013)	337
2.36.7. directed_broadcasts (ID: 06000030)	338
2.36.8. directed_broadcasts (ID: 06000031)	338
2.36.9. unknown_vlanid (ID: 06000040)	338
2.36.10. ruleset_reject_packet (ID: 06000050)	338
2.36.11. ruleset_drop_packet (ID: 06000051)	339
2.36.12. unhandled_local (ID: 06000060)	339
2.37. SESMGR	340
2.37.1. sesmgr_session_created (ID: 04900001)	340
2.37.2. sesmgr_session_denied (ID: 04900002)	340
2.37.3. sesmgr_session_removed (ID: 04900003)	340
2.37.4. sesmgr_access_set (ID: 04900004)	341
2.37.5. sesmgr_session_timeout (ID: 04900005)	341
2.37.6. sesmgr_upload_denied (ID: 04900006)	341
2.37.7. sesmgr_console_denied (ID: 04900007)	342
2.37.8. sesmgr_session_maximum_reached (ID: 04900008)	342
2.37.9. sesmgr_allocate_error (ID: 04900009)	342
2.37.10. sesmgr_session_activate (ID: 04900010)	343
2.37.11. sesmgr_session_disabled (ID: 04900011)	343
2.37.12. sesmgr_console_denied_init (ID: 04900012)	343
2.37.13. sesmgr_session_previous_removed (ID: 04900014)	344
2.37.14. sesmgr_session_access_missing (ID: 04900015)	344
2.37.15. sesmgr_session_old_removed (ID: 04900016)	344
2.37.16. sesmgr_file_error (ID: 04900017)	345
2.37.17. sesmgr_techsupport (ID: 04900018)	345
2.38. SLB	346
2.38.1. server_online (ID: 02900001)	346
2.38.2. server_offline (ID: 02900002)	346
2.39. SNMP	347
2.39.1. disallowed_sender (ID: 03100001)	347
2.39.2. invalid_snmp_community (ID: 03100002)	347
2.40. SYSTEM	348
2.40.1. demo_expired (ID: 03200020)	348
2.40.2. demo_mode (ID: 03200021)	348
2.40.3. reset_clock (ID: 03200100)	348
2.40.4. reset_clock (ID: 03200101)	349
2.40.5. invalid_ip_match_access_section (ID: 03200110)	349
2.40.6. port_bind_failed (ID: 03200300)	349
2.40.7. port_bind_failed (ID: 03200301)	350
2.40.8. port_hlm_conversion (ID: 03200302)	350
2.40.9. port_llm_conversion (ID: 03200303)	350
2.40.10. ssl_encryption_failed (ID: 03200450)	351
2.40.11. bidir_fail (ID: 03200600)	351
2.40.12. disk_cannot_remove_file (ID: 03200601)	351
2.40.13. file_open_failed (ID: 03200602)	351

2.40.14.	disk_cannot_remove (ID: 03200603)	352
2.40.15.	disk_cannot_rename (ID: 03200604)	352
2.40.16.	cfg_switch_fail (ID: 03200605)	352
2.40.17.	core_switch_fail (ID: 03200606)	353
2.40.18.	bidir_ok (ID: 03200607)	353
2.40.19.	shutdown (ID: 03201000)	353
2.40.20.	shutdown (ID: 03201010)	354
2.40.21.	shutdown (ID: 03201011)	354
2.40.22.	startup_normal (ID: 03202000)	354
2.40.23.	startup_echo (ID: 03202001)	355
2.40.24.	shutdown (ID: 03202500)	355
2.40.25.	admin_login (ID: 03203000)	355
2.40.26.	admin_logout (ID: 03203001)	356
2.40.27.	admin_login_failed (ID: 03203002)	356
2.41.	TCP_FLAG	358
2.41.1.	tcp_flags_set (ID: 03300001)	358
2.41.2.	tcp_flags_set (ID: 03300002)	358
2.41.3.	tcp_flag_set (ID: 03300003)	358
2.41.4.	tcp_flag_set (ID: 03300004)	359
2.41.5.	tcp_null_flags (ID: 03300005)	359
2.41.6.	tcp_flags_set (ID: 03300008)	359
2.41.7.	tcp_flag_set (ID: 03300009)	360
2.41.8.	unexpected_tcp_flags (ID: 03300010)	360
2.41.9.	mismatched_syn_reseat (ID: 03300011)	360
2.41.10.	mismatched_first_ack_seqno (ID: 03300012)	361
2.41.11.	mismatched_first_ack_seqno (ID: 03300013)	361
2.41.12.	rst_out_of_bounds (ID: 03300015)	362
2.41.13.	tcp_seqno_too_low (ID: 03300016)	362
2.41.14.	unacceptable_ack (ID: 03300017)	362
2.41.15.	rst_without_ack (ID: 03300018)	363
2.41.16.	tcp_seqno_too_high (ID: 03300019)	363
2.41.17.	tcp_recv_windows_drained (ID: 03300022)	364
2.41.18.	tcp_snd_windows_drained (ID: 03300023)	364
2.41.19.	tcp_get_fresocket_failed (ID: 03300024)	364
2.42.	TCP_OPT	366
2.42.1.	tcp_mss_too_low (ID: 03400001)	366
2.42.2.	tcp_mss_too_low (ID: 03400002)	366
2.42.3.	tcp_mss_too_high (ID: 03400003)	366
2.42.4.	tcp_mss_too_high (ID: 03400004)	367
2.42.5.	tcp_mss_above_log_level (ID: 03400005)	367
2.42.6.	tcp_option (ID: 03400006)	367
2.42.7.	tcp_option_strip (ID: 03400007)	368
2.42.8.	bad_tcptopt_length (ID: 03400010)	368
2.42.9.	bad_tcptopt_length (ID: 03400011)	369
2.42.10.	bad_tcptopt_length (ID: 03400012)	369
2.42.11.	tcp_mss_too_low (ID: 03400013)	369
2.42.12.	tcp_mss_too_high (ID: 03400014)	370
2.42.13.	tcp_option_disallowed (ID: 03400015)	370
2.42.14.	tcp_null_flags (ID: 03400016)	370
2.42.15.	multiple_tcp_ws_options (ID: 03400017)	371
2.42.16.	too_large_tcp_window_scale (ID: 03400018)	371
2.42.17.	mismatching_tcp_window_scale (ID: 03400019)	371
2.43.	THRESHOLD	373
2.43.1.	conn_threshold_exceeded (ID: 05300100)	373
2.43.2.	reminder_conn_threshold (ID: 05300101)	373
2.43.3.	conn_threshold_exceeded (ID: 05300102)	373
2.43.4.	failed_to_keep_connection_count (ID: 05300200)	374
2.43.5.	failed_to_keep_connection_count (ID: 05300201)	374
2.43.6.	threshold_conns_from_srcip_exceeded (ID: 05300210)	374
2.43.7.	threshold_conns_from_srcip_exceeded (ID: 05300211)	375
2.43.8.	threshold_conns_from_filter_exceeded (ID: 05300212)	375
2.43.9.	threshold_conns_from_filter_exceeded (ID: 05300213)	376
2.44.	TIMESYNC	377

2.44.1. synced_clock (ID: 03500001)	377
2.44.2. failure_communicate_with_timeservers (ID: 03500002)	377
2.44.3. clockdrift_too_high (ID: 03500003)	377
2.45. TRANSPARENCY	379
2.45.1. impossible_hw_sender_address (ID: 04400410)	379
2.45.2. enet_hw_sender_broadcast (ID: 04400411)	379
2.45.3. enet_hw_sender_broadcast (ID: 04400412)	379
2.45.4. enet_hw_sender_broadcast (ID: 04400413)	380
2.45.5. enet_hw_sender_multicast (ID: 04400414)	380
2.45.6. enet_hw_sender_multicast (ID: 04400415)	380
2.45.7. enet_hw_sender_multicast (ID: 04400416)	381
2.45.8. relay_stp_frame (ID: 04400417)	381
2.45.9. dropped_stp_frame (ID: 04400418)	381
2.45.10. invalid_stp_frame (ID: 04400419)	382
2.45.11. relay_mpls_frame (ID: 04400420)	382
2.45.12. dropped_mpls_packet (ID: 04400421)	382
2.45.13. invalid_mpls_packet (ID: 04400422)	382
2.46. USERAUTH	384
2.46.1. accounting_start (ID: 03700001)	384
2.46.2. invalid_accounting_start_server_response (ID: 03700002)	384
2.46.3. no_accounting_start_server_response (ID: 03700003)	384
2.46.4. invalid_accounting_start_server_response (ID: 03700004)	385
2.46.5. no_accounting_start_server_response (ID: 03700005)	385
2.46.6. invalid_accounting_start_server_response (ID: 03700006)	385
2.46.7. failed_to_send_accounting_stop (ID: 03700007)	386
2.46.8. accounting_stop (ID: 03700008)	386
2.46.9. invalid_accounting_stop_server_response (ID: 03700009)	387
2.46.10. no_accounting_stop_server_response (ID: 03700010)	387
2.46.11. invalid_accounting_stop_server_response (ID: 03700011)	387
2.46.12. failure_init_radius_accounting (ID: 03700012)	388
2.46.13. invalid_accounting_start_request (ID: 03700013)	388
2.46.14. no_accounting_start_server_response (ID: 03700014)	388
2.46.15. user_timeout (ID: 03700020)	389
2.46.16. group_list_too_long (ID: 03700030)	389
2.46.17. accounting_alive (ID: 03700050)	389
2.46.18. accounting_interim_failure (ID: 03700051)	390
2.46.19. no_accounting_interim_server_response (ID: 03700052)	390
2.46.20. invalid_accounting_interim_server_response (ID: 03700053)	391
2.46.21. invalid_accounting_interim_server_response (ID: 03700054)	391
2.46.22. relogin_from_new_srcip (ID: 03700100)	391
2.46.23. already_logged_in (ID: 03700101)	392
2.46.24. user_login (ID: 03700102)	392
2.46.25. bad_user_credentials (ID: 03700104)	392
2.46.26. radius_auth_timeout (ID: 03700105)	393
2.46.27. manual_logout (ID: 03700106)	393
2.46.28. userauthrules_disallowed (ID: 03700107)	393
2.46.29. challenges_not_supported (ID: 03700108)	393
2.46.30. no_shared_ciphers (ID: 03700500)	394
2.46.31. disallow_clientkeyexchange (ID: 03700501)	394
2.46.32. bad_packet_order (ID: 03700502)	394
2.46.33. bad_clienthello_msg (ID: 03700503)	395
2.46.34. bad_changecipher_msg (ID: 03700504)	395
2.46.35. bad_clientkeyexchange_msg (ID: 03700505)	395
2.46.36. bad_clientfinished_msg (ID: 03700506)	396
2.46.37. bad_alert_msg (ID: 03700507)	396
2.46.38. unknown_ssl_error (ID: 03700508)	396
2.46.39. negotiated_cipher_does_not_permit_the_chosen_certificate_size (ID: 03700509)	397
2.46.40. received_sslalert (ID: 03700510)	397
2.46.41. sent_sslalert (ID: 03700511)	397
2.47. VFS	399
2.47.1. odm_execute_action (ID: 05200002)	399
2.47.2. odm_execute_action (ID: 05200003)	399

2.47.3. odm_no_execute_action (ID: 05200004)	399
2.47.4. pkg_execute_fail (ID: 05200005)	400
2.47.5. upload_certificate_fail (ID: 05200006)	400
2.47.6. upload_certificate_fail (ID: 05200007)	400

List of Tables

1. Abbreviations	24
------------------------	----

List of Examples

1. Log Message Parameters	23
2. Conditional Log Message Parameters	23

Preface

Audience

The target audience for this reference guide consists of:

- Administrators that are responsible for configuring and managing a CorePlus installation.
- Administrators that are responsible for troubleshooting a CorePlus installation.

This guide assumes that the reader is familiar with CorePlus and understands the fundamentals of IP network security.

Notation

The following notation is used throughout this reference guide when specifying the parameters of a log message:

Angle Brackets <name> Used for specifying the *name* of a log message parameter.

Square Brackets [name] Used for specifying the *name of a conditional* log message parameter.

Example 1. Log Message Parameters

Log Message New configuration activated by user <username>, and committed via <authsystem>

Parameters authsystem
 username

Both the *authsystem* and the *username* parameters will be included.

Example 2. Conditional Log Message Parameters

Log Message Administrative user <username> logged in via <authsystem>. Access level: <access_level>

Parameters authsystem
 username
 access_level
 [userdb]
 [server_ip]
 [server_port]
 [client_ip]
 [client_port]

The *authsystem*, *username* and the *access_level* parameters will be included. The other parameters of *userdb*, *server_ip*, *server_port*, *client_ip* and *client_port* may or may not be included, depending on the context of the log message.

Abbreviations

The following abbreviations are used throughout this reference guide:

Table 1. Abbreviations

Abbreviation	Full name
ALG	Application Layer Gateway
ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
HA	High Availability
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPSec	Internet Protocol Security
L2TP	Layer 2 Tunneling Protocol
NAT	Network Address Translation
OSPF	Open Shortest Path First
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
RADIUS	Remote Authentication Dial In User Service
SAT	Static Address Translation
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCP	Transport Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTF	Unicode Transformation Format
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

Chapter 1. Introduction

- Log Message Structure, page 25
- Context Parameters, page 27
- Statistics (usage), page 31
- Severity levels, page 32

This guide is a reference for all log messages generated by CorePlus. It is designed to be a valuable information source for both management and troubleshooting.

1.1. Log Message Structure

All log messages have a common design with attributes that include category, severity and recommended actions. These attributes enable the easy filtering of log messages, either within CorePlus prior to sending them to a log receiver, or as part of analysis that takes place after the logging and storage of messages on an external log server.

The following information is provided for each specific log message:

Name The name of the log message, which is a short string, 1-6 words separated by `_`. Please note that the name *cannot* be used as a unique identification of the log message, as several log messages might share the same name.

ID The ID is a number made up of a string of 8 digits which uniquely identifies the log message. The first 3 digits identify the category to which the log message belongs.



Note

In this guide, the Name and the ID of the log message form the title of the section describing the log message.

Category Log messages are grouped into categories, where each category maps to a specific subsystem in CorePlus. For instance, the IPSEC category includes some hundreds of log messages, all related to IPsec VPN activities. Other examples of categories include ARP, DHCP, IGMP and USERAUTH.

In this guide, categories are listed as sections in Chapter 2, *Log Message Reference*.

As previously mentioned, the category is identified by the first 3 digits in the message ID. All messages in a particular category have the same first 3 digits in their ID.

Default Severity The default severity level for this log message. For a list of severity levels, please see section Section 1.4, “Severity levels”.

Log Message A brief explanation of the event that took place. This explanation often features references to parameters, enclosed in angle brackets. Example:

Administrative user <username> logged in via <authsystem>. Access level: <access_level>

**Note**

This string is only included in log messages sent to Clavister Log Receivers.

Explanation	<p>A detailed explanation of the event.</p> <p>Note that this information is only featured in this reference guide, and is never actually included in the log message.</p>
Gateway Action	<p>A short string, 1-3 words separated by _, of what action CorePlus will take. If the log message is purely informative, this is set to "None".</p>
Recommended Action	<p>A detailed recommendation of what the administrator should do if this log message is received. If the log message is purely informative, this is set to "None".</p> <p>Note that this information is only featured in this reference guide, and is never actually included in the log message.</p>
Revision	<p>The current revision of the log message. This is increased each time a log message is changed between two releases.</p>

Additional Information

Depending on the log message, the following information may also be included:

Parameters	<p>The name of the parameters that are included in this log message. If a parameter is specified within square brackets (for example [username]), then the parameter is optional and may or may not be included in the log message.</p>
Context Parameters	<p>The name of the context parameters that are included in this log message. Please see Section 1.2, "Context Parameters" for a description of all available context parameters.</p>

1.2. Context Parameters

In many cases, information regarding a certain object is featured in the log message. This can be information about, for example, a connection. In this case, the log message should, besides all the normal log message attributes, also include information about which protocol is used, source and destination IP addresses and ports (if applicable), and so on.

As the same information will be included in many log messages, these are referenced as a *Context Parameter*. So whenever a log message includes information about a connection, it will feature the CONN parameter in the Context Parameter list. This means that additional information about the connection will also be included in the log message.

A description of all available context parameters follows with an explanation of all the additional parameters. The names of the additional parameters are specified using the Syslog format.



Note

The additional parameters are formatted differently in the EFWLog format, giving them a more user friendly presentation.

ALG Module Name

An ALG is always of a certain type, for example FTP, H323 or HTTP. This parameter specifies the name of the ALG sub-module, in order to quickly distinguish which type of ALG this is.

algmod The name of the ALG sub-module.

ALG Session ID

Each ALG session has its own session ID, which uniquely identifies an ALG session. This is useful, for example, when matching the opening of an ALG session with the closure of the same ALG session.

algsesid The session ID of an ALG session.

Packet Buffer

Information about the packet buffer, which in turn contains a large number of additional objects. Certain parameters may or may not be included, depending on the type of packet buffer. For example, the TCP flags are only included if the buffer contains a TCP protocol, and the ICMP-specific parameters are only included if the buffer contains a ICMP protocol.

recvif The name of the receiving interface.

[hwsender] The sender hardware address. Valid if the protocol is ARP.

[hwdest] The destination hardware address. Valid if the protocol is ARP.

[arp] The ARP state. Valid if the protocol is ARP. Possible values: *request/reply*.

[srcip] The source IP Address. Valid if the protocol is not ARP.

[destip] The destination IP Address. Valid if the protocol is not ARP.

iphdrlen The IP header length.

[fragoffs] Fragmentation offset. Valid if the IP packet is fragmented.

[fragid] Fragmentation ID. Valid if the IP packet is fragmented.

ipproto	The IP Protocol.
ipdatalen	The IP data length.
[srcport]	The source port. Valid if the protocol is TCP or UDP.
[destport]	The destination port. Valid if the protocol is TCP or UDP.
[tcphdrln]	The TCP header length. Valid if the protocol is TCP.
[udptotlen]	The total UDP data length. Valid if the protocol is UDP.
[[tcpflag]=1]	The specific TCP flag is set. Valid if the protocol is TCP. Possible values for tcpflag: <i>syn, rst, ack, psh, fin, urg, ece, cwr</i> and <i>ns</i> .
[icmptype]	The ICMP sub-protocol name. Valid if the protocol is ICMP.
[echoid]	The ICMP echo ID. Valid if the protocol is ICMP and sub-protocol is echo.
[echoseq]	The ICMP echo sequence number. Valid if the protocol is ICMP and sub-protocol is echo.
[unreach]	The ICMP destination unreachable code. Valid if the protocol is ICMP and sub-protocol is destination unreachable.
[redirect]	The ICMP redirect code. Valid if the protocol is ICMP and sub-protocol is redirect.
[icmrcode]	The ICMP sub-protocol code. Valid if the protocol is ICMP and sub-protocol is not echo, destination unreachable or redirect.

Connection

Additional information about a connection. Certain parameters may or may not be included depending on the type and status of the connection. For example, the number of bytes sent by the originator and terminator is only included if the connection is closed.

conn	The status of the connection. Possible values: <i>open, close, closing</i> and <i>unknown</i> .
connipproto	The IP protocol used in this connection.
connrecvif	The name of the receive interface.
connsrcip	The source IP address.
[connsrcport]	The source port. Valid if the protocol is TCP or UDP.
[connsrcidt]	The source ID. Valid if the protocol is not TCP or UDP.
conndestif	The name of the destination interface.
conndestip	The destination IP address.
[conndestport]	The destination port. Valid if the protocol is TCP or UDP.
[conndestidt]	The destination ID. Valid if the protocol is not TCP or UDP.
[origsent]	The number of bytes sent by the originator in this connection. Valid if the connection is closing or closed.
[termsent]	The number of bytes sent by the terminator in this connection. Valid if the connection is closing or closed.

Deep Inspection

Specifies the name and a description of the signature that triggered this event.



Note

For Deep Inspection log messages an additional log receiver, an SMTP log receiver, can be configured. This information is only sent to log receives of that kind, and not included in the Syslog or EFWLog format

Dropped Fragments

Specifies detailed information about dropped fragments in a packet.



Note

This information is only sent in the EFWLog format

Rule Name

Specifies the name of the rule that was used when this event was triggered.

rule The name of the rule.

Rule Information

Additional information about the rule that was used when this event was triggered. Certain parameters may or may not be included, depending on the type of rule. For example, the name of an authenticated user is only included if this rule contains network objects that has user authentication information in them.

rule The name of the rule.

[satsrcrule] The name of the SAT source rule. Valid if the rule action is SAT.

[satdestrule] The name of the SAT destination rule. Valid if the rule action is SAT.

[srcusername] The name of the authenticated user in the source network object. Valid if the source network object has user authentication information.

[destusername] The name of the authenticated user in the destination network object. Valid if the destination network object has user authentication information.

User Authentication

Additional information about a user authentication event.

authrule The name of the user authentication rule.

authagent The name of the user authentication agent.

authevent The user authentication event that occurred. Possible values: *login*, *logout*, *timeout*, *disallowed_login*, *accounting* and *unknown*.

username The name of the user that triggered this event.

srcip The source IP address of the user that triggered this event.

OSPF

Additional information about OSPF.

logsection	The OSPF section Possible values: <i>packet, hello, ddesc, exchange, lsa, spf, route</i> and <i>unknown</i> .
loglevel	The log level value.

OSPF LSA

Additional information about OSPF LSA.

lsatype	The LSA type Possible values: <i>Router, network, IP summary, ASBR summary</i> and <i>AS external</i> .
lsaid	The LSA identifier.
lsaadvtr	The originating router for the LSA.

Dynamic Route

Additional information about events regarding a dynamic route.

event	The dynamic routing event that occurred. Possible values: <i>add, remove, modify, export, unexport</i> and <i>unknown</i> .
from	Originating router process.
to	Destination router process.

Route

Additional information about a route.

route	Route network.
routeiface	Route destination interface.
routegw	Route gateway.
routemetric	Route metric (cost).

1.3. Statistics (usage)

CorePlus periodically sends information about open connections and network load to its log recipients. This is sent once every hour per default.

The category for these log messages is *USAGE*, the severity level is *NOTICE*, and the log message string is *usage*. The log message looks like this in Syslog format:

conns	Number of active connections.
if<number>	The interface name, where <i>number</i> is incremented for each interface.
ip<number>	The IP address of the interface, where <i>number</i> is incremented for each interface.
tp<number>	Throughput of the interface (in Mbps - megabits per second), where <i>number</i> is incremented for each interface.

The EFWLog format includes more detailed information. The following statistics about connections is available in the EFWLog format:

- Connections opened/closed.
- Maximum/minimum number of connections.
- Current number of active connections.

The following statistics is available per interface:

- Bits in/out per second.
- Packets in/out per second.
- Packets dropped per second.

**Note**

This log messages can not be customized.

1.4. Severity levels

An event has a default severity level, based on how serious the event is. The following eight severity levels are possible, as defined by the Syslog protocol:

0 - Emergency	Emergency conditions, which most likely led to the system being unusable.
1 - Alert	Alert conditions, which affected the functionality of the unit. Needs attention immediately.
2 - Critical	Critical conditions, which affected the functionality of the unit. Action should be taken as soon as possible.
3 - Error	Error conditions, which probably affected the functionality of the unit.
4 - Warning	Warning conditions, which could affect the functionality of the unit.
5 - Notice	Normal, but significant, conditions.
6 - Informational	Informational conditions.
7 - Debug	Debug level events.

Priority in Syslog Messages

In Syslog messages the priority is indicated by the parameter **prio=*nn***.

Excluding Logged Messages

CorePlus allows the exclusion from logging of entire categories of log messages or just specific log messages. It is also possible to change the severity level of log messages so that a specific category or a specific message has the severity reset to a particular level when it is sent by CorePlus. These features are documented further in the CorePlus Administrators Guide.

Chapter 2. Log Message Reference

- ALG, page 35
- ANTIVIRUS, page 79
- ARP, page 87
- AVUPDATE, page 93
- BLACKLIST, page 96
- BUFFERS, page 99
- CONN, page 100
- DEVICEMONITOR, page 106
- DHCP, page 108
- DHCPRELAY, page 114
- DHCPSEVER, page 124
- DYNROUTING, page 133
- FRAG, page 136
- GRE, page 147
- HA, page 150
- HWM, page 159
- IDP, page 164
- IDPUPDATE, page 172
- IFACEMON, page 175
- IGMP, page 177
- IPPOOL, page 186
- IPSEC, page 192
- IP_ERROR, page 249
- IP_FLAG, page 251
- IP_OPT, page 253
- IP_PROTO, page 260
- L2TP, page 270
- LICUPDATE, page 276
- NETCON, page 277
- OSPF, page 288
- PPP, page 310

- PPPOE, page 317
- PPTP, page 318
- REASSEMBLY, page 327
- RFO, page 330
- RULE, page 336
- SESMGR, page 340
- SLB, page 346
- SNMP, page 347
- SYSTEM, page 348
- TCP_FLAG, page 358
- TCP_OPT, page 366
- THRESHOLD, page 373
- TIMESYNC, page 377
- TRANSPARENCY, page 379
- USERAUTH, page 384
- VFS, page 399



Sort Order

All log messages are sorted by their category and then by their ID number.

2.1. ALG

These log messages refer to the **ALG (Events from Application Layer Gateways)** category.

2.1.1. alg_session_open (ID: 00200001)

Default Severity	INFORMATIONAL
Log Message	ALG session opened
Explanation	A new ALG session has been opened.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.2. alg_session_closed (ID: 00200002)

Default Severity	INFORMATIONAL
Log Message	ALG session closed
Explanation	An ALG session has been closed.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.3. max_line_length_exceeded (ID: 00200003)

Default Severity	ERROR
Log Message	Maximum line length <max> exceeded, got <len> characters. Closing connection
Explanation	The maximum length of an entered line was exceeded, and the connection will be closed.
Gateway Action	close
Recommended Action	If the maximum line length is configured too low, increase it.
Revision	1
Parameters	len max
Context Parameters	ALG Module Name ALG Session ID

2.1.4. invalid_client_http_header_received (ID: 00200100)

Default Severity	WARNING
Log Message	HTTPALG: Invalid HTTP header was received from the client. Closing Connection. ALG name: <alname>.
Explanation	An invalid HTTP header was received from the client.
Gateway Action	close
Recommended Action	Research the source of this and try to find out why the client is sending an invalid header.
Revision	1
Parameters	alname
Context Parameters	ALG Module Name

ALG Session ID

2.1.5. invalid_url_format (ID: 00200101)

Default Severity	ERROR
Log Message	HTTPALG: Failed to parse the URL requested by the client: <reason>. ALG name: <alname>.
Explanation	The unit failed parsing the requested URL. The reason for this is probably because the requested URL has an invalid format, or it contains invalid UTF8 formatted characters.
Gateway Action	close
Recommended Action	Make sure that the requested URL is formatted correctly.
Revision	1
Parameters	reason alname
Context Parameters	ALG Module Name ALG Session ID

2.1.6. unknown_client_data_received (ID: 00200105)

Default Severity	WARNING
Log Message	HTTPALG: Invalid client request - unexpected data received after the the client request header. Closing connection. ALG name: <alname>.
Explanation	Data was received after the client request header, although the header specified that no such data should be sent.
Gateway Action	closing_conneccion
Recommended Action	Research the source of this, and try to find out why the client is sending an invalid request.
Revision	1
Parameters	alname
Context Parameters	ALG Module Name ALG Session ID

2.1.7. suspicious_data_received (ID: 00200106)

Default Severity	WARNING
Log Message	HTTPALG: Too much suspicious data has been received from the server. Closing the connection. ALG name: <alname>.
Explanation	The unit is configured to do content blocking, but the data from the server contains too much suspicious data. The unit can not properly determin if this data is a valid or if it should be blocked.

Gateway Action	closing_conexion
Recommended Action	Research the source of this, and try to find out why the server is sending such large amounts of suspicious data.
Revision	1
Parameters	alname
Context Parameters	ALG Module Name ALG Session ID

2.1.8. invalid_chunked_encoding (ID: 00200107)

Default Severity	WARNING
Log Message	HTTPALG: The server sent invalid chunked encoding. Closing connection. ALG name: <alname>.
Explanation	The data received from the server was sent in chunked mode, but it was not properly formatted.
Gateway Action	closing_conexion
Recommended Action	Research the source of this, and try to find out why the server is sending invalid formatted chunked data.
Revision	1
Parameters	alname
Context Parameters	ALG Module Name ALG Session ID

2.1.9. invalid_server_http_header_received (ID: 00200108)

Default Severity	WARNING
Log Message	HTTPALG: An invalid HTTP header was received from the server. Closing connection. ALG name: <alname>.
Explanation	An invalid HTTP header was received from the server.
Gateway Action	closing_conexion
Recommended Action	Research the source of this and try to find out why the server is sending an invalid header.
Revision	1
Parameters	alname
Context Parameters	ALG Module Name ALG Session ID

2.1.10. compressed_data_received (ID: 00200109)

Default Severity	ERROR
Log Message	HTTPALG: Compressed data was received from the server, although uncompressed was requested. Closing connection. ALG name: <alname>.
Explanation	The unit requested that no compressed data should be used, but the server ignored this and sent compressed data anyway. As content processing will not work if the data is compressed, the connection will be closed.
Gateway Action	close
Recommended Action	Research the source of this, and try to find out why the server is sending compressed data.
Revision	1
Parameters	alname
Context Parameters	ALG Module Name ALG Session ID

2.1.11. max_http_sessions_reached (ID: 00200110)

Default Severity	WARNING
Log Message	HTTPALG: Maximum number of HTTP sessions (<max_sessions>) for service reached. Closing connection
Explanation	The maximum number of concurrent HTTP sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Gateway Action	close
Recommended Action	If the maximum number of HTTP sessions is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.12. failed_create_new_session (ID: 00200111)

Default Severity	CRITICAL
Log Message	HTTPALG: Failed to create new HTTPALG session (out of memory)
Explanation	An attempt to create a new HTTPALG session failed, because the unit is out of memory.
Gateway Action	close
Recommended Action	Decrease the maximum allowed HTTPALG sessions, or try to free some of the RAM used.
Revision	2

Context Parameters ALG Module Name

2.1.13. failure_connect_http_server (ID: 00200112)

Default Severity ERROR

Log Message HTTPALG: Failed to connect to the HTTP Server. Closing connection. ALG name: <alname>.

Explanation The unit failed to connect to the HTTP Server, resulting in that the ALG session could not be successfully opened.

Gateway Action close

Recommended Action Verify that there is a listening HTTP Server on the specified address.

Revision 1

Parameters alname

Context Parameters ALG Module Name
ALG Session ID

2.1.14. content_type_mismatch (ID: 00200113)

Default Severity NOTICE

Log Message HTTPALG: Content type mismatch in file <filename>. Identified filetype <filetype>

Explanation The filetype of the file does not match the actual content type. As there is a content type mismatch, data is discarded.

Gateway Action block_data

Recommended Action None.

Revision 1

Parameters filename
filetype
contenttype

Context Parameters ALG Module Name
ALG Session ID

2.1.15. wcf_override_full (ID: 00200114)

Default Severity ERROR

Log Message HTTPALG: WCF override cache full

Explanation The WCF override hash is full. The oldest least used value will be replaced.

Gateway Action replace

Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.16. content_filtering_disabled (ID: 00200115)

Default Severity	ERROR
Log Message	HTTPALG: Web Content Filtering disabled
Explanation	Web Content Filtering has been disabled due to license restriction.
Gateway Action	no_valid_license
Recommended Action	Extend valid time for Content Filtering.
Revision	2
Context Parameters	ALG Module Name

2.1.17. max_download_size_reached (ID: 00200116)

Default Severity	WARNING
Log Message	HTTPALG: The file <filename> with file size <filesize>kB exceeds the maximum allowed download size <max_download_size>kB. Closing connection
Explanation	The data received from the server exceeds the maximum allowed download file size, the request is rejected and the connection is closed.
Gateway Action	close
Recommended Action	If the configurable maximum download size is too low, increase it.
Revision	2
Parameters	filename filesize max_download_size
Context Parameters	ALG Module Name ALG Session ID

2.1.18. blocked_filetype (ID: 00200117)

Default Severity	NOTICE
Log Message	HTTPALG: Requested file:<filename> is blocked as this file is identified as type <filetype>, which is in block list.
Explanation	The file is present in the block list. It will be blocked as per configuration.
Gateway Action	block

Recommended Action	If this file should be allowed, update the ALLOW/BLOCK list.
Revision	2
Parameters	filename filetype
Context Parameters	ALG Module Name ALG Session ID

2.1.19. out_of_mem (ID: 00200118)

Default Severity	CRITICAL
Log Message	HTTPALG: Failed to allocate memory
Explanation	The unit does not have enough available RAM. WCF could not allocate memory for override functionality.
Gateway Action	none
Recommended Action	Try to free up some RAM by changing configuration parameters.
Revision	1
Context Parameters	ALG Module Name

2.1.20. wcf_servers_unreachable (ID: 00200119)

Default Severity	CRITICAL
Log Message	HTTPALG: Failed to connect to web content servers
Explanation	Web Content Filtering was unable to connect to the Web Content Filtering servers. Verify that the unit has been configured with Internet access.
Gateway Action	none
Recommended Action	Check_configuration.
Revision	2
Context Parameters	ALG Module Name

2.1.21. wcf_srv_connection_error (ID: 00200120)

Default Severity	ERROR
Log Message	HTTPALG: HTTP request not validated by Web Content Filter and allowed.
Explanation	The Web Content Filtering servers could not be contacted. The request has been allowed since fail-mode parameter is in allow mode.
Gateway Action	allow

Recommended Action	Investigate why the Web Content Filtering servers cannot be reached.
Revision	1
Parameters	algnam
Context Parameters	ALG Module Name ALG Session ID

2.1.22. wcf_server_unreachable (ID: 00200121)

Default Severity	ERROR
Log Message	HTTPALG: Failed to connect to web content server <failedserver>
Explanation	Web Content Filtering was unable to connect to the Web Content Filtering server. The system will try to contact one of the backup servers.
Gateway Action	switching_server
Recommended Action	None.
Revision	1
Parameters	failedserver
Context Parameters	ALG Module Name

2.1.23. wcf_connecting (ID: 00200122)

Default Severity	INFORMATIONAL
Log Message	HTTPALG:Connecting to web content server <server>
Explanation	Connecting to Web Content Filtering server.
Gateway Action	connecting
Recommended Action	None.
Revision	1
Parameters	server
Context Parameters	ALG Module Name

2.1.24. wcf_server_connected (ID: 00200123)

Default Severity	INFORMATIONAL
Log Message	HTTPALG: Web content server <server> connected
Explanation	The connection with the Web Content server has been established. .
Gateway Action	None

Recommended Action	None.
Revision	1
Parameters	server
Context Parameters	ALG Module Name

2.1.25. wcf_primary_fallback (ID: 00200124)

Default Severity	INFORMATIONAL
Log Message	HTTPALG: Falling back from secondary servers to primary server
Explanation	Web Content Filtering falls back to primary server after 60 minutes.
Gateway Action	none
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.26. request_url (ID: 00200125)

Default Severity	NOTICE
Log Message	HTTPALG: Requesting URL <url>. Categories: <categories>. Audit: <audit>. Override: <override>. ALG name: <alname>.
Explanation	The URL has been requested.
Gateway Action	allow
Recommended Action	None.
Revision	2
Parameters	categories audit override url alname
Context Parameters	Connection Connection ALG Module Name ALG Session ID

2.1.27. request_url (ID: 00200126)

Default Severity	NOTICE
Log Message	HTTPALG: Requesting URL <url>. Categories: <categories>. Audit: <audit>. Override: <override>. ALG name: <alname>.

Explanation	The URL has been requested.
Gateway Action	block
Recommended Action	None.
Revision	2
Parameters	categories audit override url alname
Context Parameters	Connection Connection ALG Module Name ALG Session ID

2.1.28. request_url (ID: 00200129)

Default Severity	NOTICE
Log Message	HTTPALG: Requesting URL <url>. Categories: <categories>. Audit: <audit>. Override: <override>. ALG name: <alname>.
Explanation	The URL has been requested.
Gateway Action	allow_audit_mode
Recommended Action	None.
Revision	2
Parameters	categories audit override url alname
Context Parameters	Connection Connection ALG Module Name ALG Session ID

2.1.29. restricted_site_notice (ID: 00200132)

Default Severity	WARNING
Log Message	HTTPALG: User requests the forbidden URL <url>, eventhough Restricted Site Notice was applied. ALG name: <alname>.
Explanation	The URL has been requested and the categories are forbidden. Restricted Site Notice was applied.
Gateway Action	allow
Recommended Action	Disable the RESTRICTED_SITE_NOTICE mode of parameter CATEGORIES for this ALG.

Revision	2
Parameters	url alname
Context Parameters	Connection Connection ALG Module Name ALG Session ID

2.1.30. url_reclassification_request (ID: 00200133)

Default Severity	WARNING
Log Message	HTTPALG: Reclassification request for URL <url>. New Category <newcat>. ALG name: <alname>.
Explanation	The user has requested a category reclassification for the URL.
Gateway Action	allow
Recommended Action	Disable the ALLOW_RECLASSIFICATION mode of parameter CATEGORIES for this ALG.
Revision	2
Parameters	newcat url alname
Context Parameters	Connection Connection ALG Module Name ALG Session ID

2.1.31. max_smtp_sessions_reached (ID: 00200150)

Default Severity	WARNING
Log Message	SMTPALG: Maximum number of SMTP sessions (<max_sessions>) for service reached. Closing connection
Explanation	The maximum number of concurrent SMTP sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Gateway Action	close
Recommended Action	If the maximum number of SMTP sessions is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.32. maximum_email_per_minute_reached (ID:

00200151)

Default Severity	WARNING
Log Message	SMTPALG: Maximum number of emails per client and minute reached.
Explanation	Client is trying to send emails at a rate higher than the configured value.
Gateway Action	session_rejected
Recommended Action	This can be a possible DOS attack.
Revision	2
Parameters	sender_email_address
Context Parameters	ALG Module Name ALG Session ID

2.1.33. failed_create_new_session (ID: 00200152)

Default Severity	CRITICAL
Log Message	SMTPALG: Failed to create new SMTPALG session (out of memory)
Explanation	An attempt to create a new SMTPALG session failed. The unit has run out of memory.
Gateway Action	close
Recommended Action	Decrease the maximum allowed SMTPALG sessions, or try to free some of the RAM used.
Revision	2
Context Parameters	ALG Module Name

2.1.34. failed_connect_smtp_server (ID: 00200153)

Default Severity	ERROR
Log Message	SMTPALG: Failed to connect to the SMTP Server. Closing the connection.
Explanation	The SMTP ALG could not connect to the receiving SMTP server, resulting in that the ALG session could not be successfully opened.
Gateway Action	close
Recommended Action	None.
Revision	3
Context Parameters	ALG Module Name ALG Session ID

2.1.35. invalid_server_response (ID: 00200155)

Default Severity	ERROR
Log Message	SMTPALG: Could not parse server response code
Explanation	The SMTP ALG failed to parse the SMTP response code from server.
Gateway Action	close
Recommended Action	If possible, verify response codes sent from server.
Revision	3
Context Parameters	Connection ALG Module Name ALG Session ID

2.1.36. sender_email_id_mismatched (ID: 00200157)

Default Severity	WARNING
Log Message	SMTPALG: Mismatching sender address
Explanation	The SMTP "MAIL FROM:" command does not match the "From:" header. The transaction will be denied.
Gateway Action	reject
Recommended Action	Disable the Verify E-Mail Sender ID setting if you experience that valid e-mails are being wrongly blocked.
Revision	3
Parameters	sender_email_address recipient_email_addresses data_sender_address
Context Parameters	ALG Module Name ALG Session ID

2.1.37. sender_email_id_is_in_blacklist (ID: 00200158)

Default Severity	WARNING
Log Message	SMTPALG: Sender e-mail address is in Black List
Explanation	Since "MAIL FROM:" Email Id is in Black List, SMTP ALG rejected the Client request.
Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	sender_email_address

Context Parameters	ALG Module Name ALG Session ID
---------------------------	-----------------------------------

2.1.38. recipient_email_id_in_blacklist (ID: 00200159)

Default Severity	WARNING
Log Message	SMTPALG: Recipient e-mail address is in Black List
Explanation	Since "RCPT TO:" e-mail address is in Black List, SMTP ALG rejected the client request.
Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.39. some_recipient_email_ids_are_in_blocklist (ID: 00200160)

Default Severity	WARNING
Log Message	SMTPALG: Some recipients email id are in Black List
Explanation	Since some "RCPT TO:" Email ids are in Black List, SMTP ALG has blocked mail to those recipients.
Gateway Action	reject
Recommended Action	Emails can be forwarded only to the Non-Black List users.
Revision	1
Parameters	sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.40. base64_decode_failed (ID: 00200164)

Default Severity	ERROR
Log Message	SMTPALG: Base 64 decode failed. Attachment blocked
Explanation	The base64 encoded attachment could not be decoded. This can occur if the email sender sends incorrectly formatted data. The attachment has been blocked.

Gateway Action	block_allow
Recommended Action	Research how the sender is encoding the data.
Revision	2
Parameters	filename filetype sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.41. base64_decode_failed (ID: 00200165)

Default Severity	ERROR
Log Message	SMTPALG: Base 64 decode failed. Attachment is allowed
Explanation	The data sent to Base64 decoding failed. This can occur if the email sender sends incorrectly formatted data. Fail-mode is set to allow so data will be forwarded.
Gateway Action	allow_block
Recommended Action	Research how the sender is encoding the data.
Revision	2
Parameters	filename filetype sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.42. blocked_filetype (ID: 00200166)

Default Severity	NOTICE
Log Message	SMTPALG: Requested file:<filename> is blocked as this file is identified as type <filetype>, which is in block list.
Explanation	The file is present in the block list. It will be blocked as per configuration.
Gateway Action	block
Recommended Action	If this file should be allowed, update the ALLOW/BLOCK list.
Revision	2
Parameters	filename filetype sender_email_address recipient_email_addresses

Context Parameters	ALG Module Name ALG Session ID
---------------------------	-----------------------------------

2.1.43. content_type_mismatch (ID: 00200167)

Default Severity	WARNING
Log Message	SMTPALG: Content type mismatch in file <filename>. Identified filetype <filetype>
Explanation	The filetype of the file does not match the actual content type. As there is a content type mismatch, data is discarded.
Gateway Action	block_data
Recommended Action	None.
Revision	4
Parameters	filename filetype sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.44. max_email_size_reached (ID: 00200170)

Default Severity	WARNING
Log Message	SMTPALG: Maximum email size limit <max_email_size>kb reached
Explanation	Email body and all attachments size of email has crossed the limitation.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	sender_email_address recipient_email_addresses max_email_size
Context Parameters	ALG Module Name ALG Session ID

2.1.45. content_type_mismatch_mimecheck_disabled (ID: 00200171)

Default Severity	NOTICE
Log Message	SMTPALG: Content type mismatch found for the file <filename>. It is identified as type <filetype> file

Explanation	Received type of data in the packet and its actual type do not match. As there is a mismatch and mime type check is disabled, the data will be allowed.
Gateway Action	allow
Recommended Action	Content type should be matched.
Revision	3
Parameters	filename filetype sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.46. all_recipient_email_ids_are_in_blocklist (ID: 00200172)

Default Severity	WARNING
Log Message	SMTPALG: All recipients e-mail addresses are in Black List
Explanation	Since "RCPT TO:" email ids are in Black List, SMTP ALG rejected the client request.
Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.47. out_of_memory (ID: 00200175)

Default Severity	ALERT
Log Message	SMTPALG: Failed to allocate memory (out of memory)
Explanation	An attempt to allocate memory failed.
Gateway Action	close
Recommended Action	Try to free up unwanted memory.
Revision	3
Context Parameters	ALG Module Name ALG Session ID

2.1.48. invalid_end_of_mail (ID: 00200176)

Default Severity	WARNING
Log Message	SMTPALG: Invalid end of mail "\\n.\\n" received.
Explanation	The client is sending invalid end of mail. Transaction will be terminated.
Gateway Action	block
Recommended Action	Research how the client is sending invalid end of mail.
Revision	1
Parameters	sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.1.49. dnsbl_init_error (ID: 00200177)

Default Severity	ERROR
Log Message	DNSbl internal error
Explanation	The email could not be checked for spam. Email will be processed without spam checks.
Gateway Action	none
Recommended Action	None.
Revision	2
Context Parameters	ALG Module Name ALG Session ID

2.1.50. cmd_too_long (ID: 00200179)

Default Severity	ERROR
Log Message	SMTPALG: Command line too long
Explanation	The SMTP Command line exceeds the maximum command length of 712 characters. (RFC 2821 Ch. 4.5.3.1 says 512).
Gateway Action	reject
Recommended Action	None.
Revision	2
Context Parameters	ALG Module Name ALG Session ID

2.1.51. cmd_empty (ID: 00200180)

Default Severity	DEBUG
Log Message	SMTPALG: Received empty command.
Explanation	The SMTP command line was empty. Ignoring command.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.52. failed_send_reply_code (ID: 00200181)

Default Severity	ERROR
Log Message	SMTPALG: Could not send error code to client
Explanation	The SMTP ALG failed to send an error response code to the client.
Gateway Action	none
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.53. smtp_no_header (ID: 00200184)

Default Severity	WARNING
Log Message	SMTPALG: Email without SMTP headers received
Explanation	The SMTP ALG received an email without headers.
Gateway Action	allow
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.54. unsupported_extension (ID: 00200185)

Default Severity	INFORMATIONAL
Log Message	SMTPALG: Removed capability <capa> from EHLO response

Explanation	The SMTP ALG removed the [capa] capability from the EHLO response since the ALG does not support the specified extension.
Gateway Action	capability_removed
Recommended Action	None.
Revision	1
Parameters	capa
Context Parameters	ALG Module Name ALG Session ID

2.1.55. cmd_pipelined (ID: 00200186)

Default Severity	ERROR
Log Message	SMTPALG: Received pipelined request.
Explanation	The SMTP ALG does not support pipelined requests. The appearance of this log message indicates that the client used PIPELINING even though it was removed from capability list.
Gateway Action	reject
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.56. smtp_state_violation (ID: 00200190)

Default Severity	WARNING
Log Message	SMTPALG: State violation: <violation>.
Explanation	The client sent an invalid sequence of commands. The protocol violation is explained by the [violation] parameter.
Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	violation
Context Parameters	Connection ALG Module Name ALG Session ID

2.1.57. illegal_data_direction (ID: 00200202)

Default Severity	ERROR
-------------------------	-------

Log Message	FTPALG: TCP data from <peer> not allowed in this direction. Closing connection
Explanation	TCP Data was sent in an invalid direction, and the connection will be closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Rule Information Connection

2.1.58. hybrid_data (ID: 00200206)

Default Severity	INFORMATIONAL
Log Message	FTPALG: Hybrid connection made
Explanation	A hybrid connection was successfully created.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID Rule Information Connection

2.1.59. hybrid_data (ID: 00200209)

Default Severity	INFORMATIONAL
Log Message	FTPALG: Hybrid data channel closed
Explanation	A hybrid data channel was closed.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID Rule Information Connection

2.1.60. illegal_chars (ID: 00200210)

Default Severity	WARNING
Log Message	FTPALG: 8 bit characters in control channel from <peer> not allowed. Closing connection
Explanation	8 bit characters were discovered in the control channel. This is not allowed according to the FTPALG configuration, and the connection will be closed.
Gateway Action	close
Recommended Action	If 8 bit characters should be allowed, modify the FTPALG configuration.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.61. control_chars (ID: 00200211)

Default Severity	WARNING
Log Message	FTPALG: Unexpected telnet control chars in control channel from <peer>. Closing connection
Explanation	Unexpected telnet control characters were discovered in the control channel. This is not allowed according to the FTPALG configuration, and the connection will be closed.
Gateway Action	close
Recommended Action	If unknown commands should be allowed, modify the FTPALG configuration.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.62. illegal_command (ID: 00200212)

Default Severity	WARNING
Log Message	FTPALG: Failed to parse command from <peer> as a FTP command. String=<string>. Closing connection
Explanation	An invalid command was received on the control channel. This is not allowed, and the connection will be closed.
Gateway Action	close

Recommended Action	If unknown commands should be allowed, modify the FTPALG configuration.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.63. illegal_command (ID: 00200213)

Default Severity	WARNING
Log Message	FTPALG: Failed to parse command from <peer> as a FTP command. String=<string>. Rejecting command
Explanation	An invalid command was received on the control channel. This is allowed, but the command will be rejected as it is not understood.
Gateway Action	rejecting_command
Recommended Action	If unknown commands should not be allowed, modify the FTPALG configuration.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.64. port_command_disabled (ID: 00200214)

Default Severity	WARNING
Log Message	FTPALG: PORT command not allowed from <peer>. Rejecting command
Explanation	The client tried to issue a "PORT" command, which is not valid since the client is not allowed to do active FTP. The command will be rejected.
Gateway Action	rejecting_command
Recommended Action	If the client should be allowed to do active FTP, modify the FTPALG configuration.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.65. illegal_command (ID: 00200215)

Default Severity	WARNING
Log Message	FTPALG: Failed to parse PORT parameters from <peer>. String=<string>. Closing connection
Explanation	Invalid parameters to the "PORT" command were received. The connection will be closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.66. illegal_ip_address (ID: 00200216)

Default Severity	CRITICAL
Log Message	FTPALG: Illegal PORT command from <peer>, bad IP address <ip4addr>. String=<string>. Rejecting command
Explanation	An illegal "PORT" command was received from the client. It requests that the server should connect to another IP that it's own. This is not allowed, and the command will be rejected.
Gateway Action	rejecting_command
Recommended Action	The FTP client could be compromised, and should not be trusted.
Revision	1
Parameters	peer ip4addr string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.67. illegal_port_number (ID: 00200217)

Default Severity	CRITICAL
Log Message	FTPALG: Illegal PORT command from <peer>, port <port> not allowed. String=<string>. Rejecting command
Explanation	An illegal "PORT" command was received from the client. It requests that the server should connect to a port which is out of range. This is

	not allowed, and the command will be rejected.
Gateway Action	rejecting_command
Recommended Action	The FTP client could be compromised, and should not be trusted.
Revision	1
Parameters	peer port string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.68. failed_to_create_connection1 (ID: 00200218)

Default Severity	ERROR
Log Message	FTPALG: Failed to create connection(1). Connection: <connection>. String=<string>
Explanation	An error occurred when creating a data connection from the server to client. This could possibly be a result of lack of memory.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	peer connection string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.69. illegal_command (ID: 00200219)

Default Severity	WARNING
Log Message	FTPALG: SITE EXEC from <peer> not allowed, rejecting command
Explanation	The client tried to issue a "SITE EXEC" command, which is not valid since the client is not allowed to do this. The command will be rejected.
Gateway Action	rejecting_command
Recommended Action	If the client should be allowed to do issue "SITE EXEC" commands, modify the FTPALG configuration.
Revision	1
Parameters	peer

Context Parameters	ALG Module Name ALG Session ID Connection
---------------------------	---

2.1.70. illegal_direction1 (ID: 00200220)

Default Severity	WARNING
Log Message	FTPALG: Illegal direction for command(1), peer=<peer>. Closing connection.
Explanation	A command was sent in an invalid direction, and the connection will be closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.71. illegal_direction2 (ID: 00200221)

Default Severity	WARNING
Log Message	FTPALG: Illegal direction for command(2), peer=<peer>. Closing connection.
Explanation	A command was sent in an invalid direction, and the connection will be closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.72. illegal_option (ID: 00200222)

Default Severity	WARNING
Log Message	FTPALG: Invalid OPTS argument from <peer>. String=<string>. Rejecting command.
Explanation	An invalid OPTS argument was received. The argument does not start with an alphabetic letter, and the command will be rejected.

Gateway Action	rejecting_command
Recommended Action	None.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.73. illegal_option (ID: 00200223)

Default Severity	WARNING
Log Message	FTPALG: Disallowed OPTS argument from <peer>. String:<string>. Rejecting command.
Explanation	A disallowed OPTS argument was received, and the command will be rejected.
Gateway Action	rejecting_command
Recommended Action	None.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.74. unknown_option (ID: 00200224)

Default Severity	WARNING
Log Message	FTPALG: Unknown OPTS argument from <peer>. String=<string>. Rejecting command.
Explanation	An unknown OPTS argument was received, and the command will be rejected.
Gateway Action	rejecting_command
Recommended Action	If unknown commands should be allowed, modify the FTPALG configuration.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.75. illegal_command (ID: 00200225)

Default Severity	WARNING
Log Message	FTPALG: Illegal command from <peer>. String=<string>. Rejecting command.
Explanation	An illegal command was received, and the command will be rejected.
Gateway Action	rejecting_command
Recommended Action	None.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.76. unknown_command (ID: 00200226)

Default Severity	WARNING
Log Message	FTPALG: Unknown command from <peer>. String=<string>. Rejecting command.
Explanation	An unknown command was received, and the command will be rejected.
Gateway Action	rejecting_command
Recommended Action	If unknown commands should be allowed, modify the FTPALG configuration.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.77. illegal_reply (ID: 00200228)

Default Severity	WARNING
Log Message	FTPALG: Illegal numerical reply (<reply>) from <peer>. String=<string>. Closing connection.
Explanation	An illegal numerical reply was received from server, and the connection will be closed.
Gateway Action	close

Recommended Action	None.
Revision	1
Parameters	peer reply string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.78. illegal_reply (ID: 00200230)

Default Severity	WARNING
Log Message	FTPALG: Illegal multiline response (<reply>) from <peer>. String=<string>. Closing connection.
Explanation	An illegal multiline response was received from server, and the connection will be closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer reply string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.79. illegal_reply (ID: 00200231)

Default Severity	WARNING
Log Message	FTPALG: Unsolicited 227 (passive mode) response from <peer>. String=<string>. Closing connection.
Explanation	An illegal response was received from the server, and the connection is closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.80. illegal_reply (ID: 00200232)

Default Severity	WARNING
Log Message	FTPALG: Reply 229 (extended passive mode) from <peer> is not allowed. String=<string>. Closing connection.
Explanation	An illegal response was received from the server, and the connection is closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.81. bad_port (ID: 00200233)

Default Severity	CRITICAL
Log Message	FTPALG: Bad port <port> from <peer>, should be within the range (<range>). String=<string>. Closing connection.
Explanation	An illegal "PORT" command was received from the server. It requests that the client should connect to a port which is out of range. This is not allowed, and the connection will be closed.
Gateway Action	close
Recommended Action	The FTP server could be compromised, and should not be trusted.
Revision	1
Parameters	peer port range string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.82. bad_ip (ID: 00200234)

Default Severity	CRITICAL
Log Message	FTPALG: Invalid IP <ip4addr>, Server IP is <ip4addr_server>. String=<string>. Closing connection.
Explanation	The FTP Server requests that the client should connect to another IP

	that it's own. This is not allowed, and the connection will be closed.
Gateway Action	close
Recommended Action	The FTP server could be compromised, and should not be trusted.
Revision	1
Parameters	peer ip4addr ip4addr_server string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.83. failed_to_create_connection2 (ID: 00200235)

Default Severity	ERROR
Log Message	FTPALG: Failed to create connection(2) Peer=<peer> Connection=<connection>. String=<string>.
Explanation	An error occurred when creating a data connection from the client to server. This could possibly be a result of lack of memory.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	peer connection string
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.84. failed_to_create_server_data_connection (ID: 00200236)

Default Severity	ERROR
Log Message	FTPALG: Failed to create server data connection. Peer=<peer> Connection=<connection>
Explanation	An error occurred when creating server data connection.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	peer

	connection
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.85. failed_to_send_port (ID: 00200237)

Default Severity	WARNING
Log Message	FTPALG: Failed to send port. Peer=<peer>
Explanation	An error occured when trying to send the "PORT" command to the server.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.86. failed_to_register_rawconn (ID: 00200238)

Default Severity	ERROR
Log Message	FTPALG: Internal Error - failed to register eventhandler. Closing connection
Explanation	An internal error occured when registering an eventhandler, and the connection will be closed.
Gateway Action	close
Recommended Action	Contact the support.
Revision	1
Context Parameters	ALG Module Name

2.1.87. failed_to_merge_conns (ID: 00200239)

Default Severity	ERROR
Log Message	FTPALG: Internal Error - failed to merge conns. Closing connection
Explanation	An internal error occured when two connections were being merged into one, and the connection will be closed.
Gateway Action	close
Recommended Action	Contact the support.

Revision	1
Context Parameters	ALG Module Name

2.1.88. max_ftp_sessions_reached (ID: 00200241)

Default Severity	WARNING
Log Message	FTPALG: Maximum number of FTP sessions (<max_sessions>) for service reached. Closing connection
Explanation	The maximum number of concurrent FTP sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Gateway Action	close
Recommended Action	If the maximum number of FTP sessions is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.89. failed_create_new_session (ID: 00200242)

Default Severity	ERROR
Log Message	FTPALG: Failed to create new FTPALG session (out of memory)
Explanation	An attempt to create a new FTPALG session failed, because the unit is out of memory.
Gateway Action	close
Recommended Action	Decrease the maximum allowed FTPALG sessions, or try to free some of the RAM used.
Revision	1
Context Parameters	ALG Module Name

2.1.90. failure_connect_ftp_server (ID: 00200243)

Default Severity	ERROR
Log Message	FTPALG: Failed to connect to the FTP Server. Closing connection
Explanation	The unit failed to connect to the FTP Server, resulting in that the ALG session could not be successfully opened.
Gateway Action	close
Recommended Action	Verify that there is a listening FTP Server on the specified address.
Revision	1

Context Parameters	ALG Module Name ALG Session ID
---------------------------	-----------------------------------

2.1.91. content_type_mismatch (ID: 00200250)

Default Severity	NOTICE
Log Message	FTPALG: Content type mismatch in file <filename>. Identified filetype <filetype>
Explanation	The filetype of the file does not match the actual content type. As there is a content type mismatch, data is discarded.
Gateway Action	data_blocked_control_and_data_channel_closed
Recommended Action	None.
Revision	1
Parameters	filename filetype
Context Parameters	ALG Module Name ALG Session ID

2.1.92. failed_to_send_command (ID: 00200251)

Default Severity	NOTICE
Log Message	FTPALG:Failed to send the command.
Explanation	The command sent by the ALG to the server could not be sent.
Gateway Action	none
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.93. resumed_compressed_file_transfer (ID: 00200252)

Default Severity	WARNING
Log Message	FTPALG: The file <filename> (File type: <filetype>) cannot be sent to antivirus scan engine.
Explanation	The data cannot be sent to AVSE for scanning since file transfer begins from within the middle of the file. The scanning process will fail for compressed files.
Gateway Action	data_blocked_control_and_data_channel_closed
Recommended Action	Change fail mode setting to allow, if resumed file transfers of compressed files should be allowed.

Revision	2
Parameters	filename filetype
Context Parameters	ALG Module Name ALG Session ID

2.1.94. blocked_filetype (ID: 00200253)

Default Severity	NOTICE
Log Message	FTPALG: Requested file:<filename> is blocked as this file is identified as type <filetype>, which is in block list.
Explanation	The file is present in the block list. It will be blocked as per configuration.
Gateway Action	data_blocked_control_and_data_channel_closed
Recommended Action	If this file should be allowed, update the ALLOW/BLOCK list.
Revision	2
Parameters	filename filetype
Context Parameters	ALG Module Name ALG Session ID

2.1.95. resumed_compressed_file_transfer (ID: 00200254)

Default Severity	WARNING
Log Message	FTPALG: The file <filename> (File type: <filetype>) cannot be sent to antivirus scan engine.
Explanation	Decompression module cannot decompress a file that has been resumed. The file is allowed without any further scanning since Fail Mode is Allow.
Gateway Action	allow_data_without_scan
Recommended Action	Update Fail-Mode parameter if the file should be blocked.
Revision	2
Parameters	filename filetype
Context Parameters	ALG Module Name ALG Session ID

2.1.96. failed_to_send_response_code (ID: 00200255)

Default Severity	NOTICE
-------------------------	--------

Log Message	FTPALG:Failed to send the response code.
Explanation	The FTP ALG could not send the correct response code to the client.
Gateway Action	none
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.97. illegal_command (ID: 00200267)

Default Severity	WARNING
Log Message	FTPALG: REST from <peer> not allowed, rejecting command
Explanation	The client tried to issue a "REST" command, which is not valid since the client is not allowed to do this. The command will be rejected.
Gateway Action	rejecting_command
Recommended Action	If the client should be allowed to do issue "REST" commands, modify the FTPALG configuration.
Revision	1
Parameters	filename peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.98. unknown_state (ID: 00200300)

Default Severity	WARNING
Log Message	H323ALG: H.225 parser is in unknown state
Explanation	The H.225 parser failed to parse the H.225 message. The ALG session will be closed.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	peer state
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.99. invalid_message (ID: 00200301)

Default Severity	WARNING
Log Message	H323ALG: An invalid message was received from peer
Explanation	An invalid message was received from the peer. The ALG session will be closed.
Gateway Action	closing_session
Recommended Action	None.
Revision	2
Parameters	peer message state
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.100. decode_failed (ID: 00200302)

Default Severity	WARNING
Log Message	H323ALG: Decoding of message from peer failed. Closing session
Explanation	The H.225 parser failed to decode the H.225 message. The ALG session will be closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer message_type
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.101. encode_failed (ID: 00200303)

Default Severity	WARNING
Log Message	H323ALG: Encoding of message from peer failed. Closing session
Explanation	The ASN.1 encoder failed to encode the message. The ALG session will be closed.
Gateway Action	close
Recommended Action	None.
Revision	1

Parameters	peer message_type
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.102. encode_failed (ID: 00200304)

Default Severity	WARNING
Log Message	H323ALG: Failed before encoding message from peer. Closing session
Explanation	The ASN.1 encoder failed to allocate memory used for encoding of the message. The ALG session will be closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer message_type
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.103. encode_failed (ID: 00200305)

Default Severity	WARNING
Log Message	H323ALG: Failed after encoding message from peer. Closing session
Explanation	The ASN.1 encoder failed to encode the message properly. The ALG session will be closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer message_type
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.104. decode_failed (ID: 00200306)

Default Severity	WARNING
Log Message	H323ALG: Failed before encoding H.245 message. Closing

	connection
Explanation	The H.245 encoder failed to allocate memory used for encoding of the message. The ALG session will be closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.105. encode_failed (ID: 00200307)

Default Severity	WARNING
Log Message	H323ALG: Failed after encoding H.245 message. Closing connection
Explanation	The H.245 encoder failed to encode the message. The ALG session will be closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.106. max_tcp_data_connections_exceeded (ID: 00200308)

Default Severity	WARNING
Log Message	H323ALG: Maximum number of TCP data channels exceeded
Explanation	The maximum number of concurrent TCP data channels has been reached for this session.
Gateway Action	None
Recommended Action	If the maximum number of TCP data channels per session is too low, increase it.
Revision	1
Parameters	max_channels
Context Parameters	ALG Module Name ALG Session ID

Connection

2.1.107. max_connections_per_call_exceeded (ID: 00200309)

Default Severity	WARNING
Log Message	H323ALG: No more connections allowed for this call
Explanation	The maximum number of concurrent logical channels (calls) has been reached for this session.
Gateway Action	None
Recommended Action	If the maximum number of concurrent logical channels (calls) per session is too low, increase it.
Revision	1
Parameters	max_connections
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.108. ignoring_channel (ID: 00200310)

Default Severity	WARNING
Log Message	H323ALG: Ignoring mediaChannel info in openLogicalChannel
Explanation	Media channel information in the openLogicalChannel message is not handled.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.109. com_mode_response_message_not_translated (ID: 00200311)

Default Severity	WARNING
Log Message	H323ALG: CommunicationModeResponse not translated.
Explanation	The H.245 Communication Mode Response message is not translated.

Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.1.110. max_h323_session_reached (ID: 00200312)

Default Severity	WARNING
Log Message	H323ALG: Maximum number of H.323 sessions (<max_sessions>) for service reached. Closing connection.
Explanation	The maximum number of concurrent H.323 sessions has been reached for this service. No more sessions can be opened before old sessions have been released.
Gateway Action	close
Recommended Action	If the maximum number of H.323 session is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.111. failed_create_new_session (ID: 00200313)

Default Severity	WARNING
Log Message	H323ALG: Failed to create new H.323 session (out of memory)
Explanation	Could not create a new H.323 session due to lack of memory. No more sessions can be created unless the system increases the amount of free memory.
Gateway Action	close
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.112. max_h323_gk_sessions_reached (ID: 00200314)

Default Severity	WARNING
Log Message	H323ALG: Maximum number of H.323 gatekeeper sessions for service reached

Explanation	The maximum number of concurrent H.323 gatekeeper sessions has been reached for this service. Connection will be closed.
Gateway Action	close
Recommended Action	If the maximum number of concurrent H.323 gatekeeper sessions is too low, increase it.
Revision	1
Parameters	max_sessions
Context Parameters	ALG Module Name

2.1.113. failed_create_new_session (ID: 00200315)

Default Severity	WARNING
Log Message	H323ALG: Failed to create new gatekeeper session (out of memory)
Explanation	Could not create a new H.323 gatekeeper session due to lack of memory. No more sessions can be created unless the system increases the amount of free memory.
Gateway Action	close
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name

2.1.114. failure_connect_h323_server (ID: 00200316)

Default Severity	ERROR
Log Message	H323ALG: Failed to connect to the H.323 Server. Closing connection
Explanation	The unit failed to connect to the H.323 Server, resulting in that the ALG session could not open successfully.
Gateway Action	close
Recommended Action	Verify that there is a listening H.323 Server on the specified address.
Revision	1
Context Parameters	ALG Module Name ALG Session ID

2.1.115. com_mode_command_message_not_translated (ID: 00200317)

Default Severity	WARNING
Log Message	H323ALG: CommunicationModeCommand not translated.

Explanation	The H.245 Communication Mode Command message is not translated.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	peer
Context Parameters	ALG Module Name ALG Session ID Connection

2.2. ANTIVIRUS

These log messages refer to the **ANTIVIRUS (Anti-virus related events)** category.

2.2.1. virus_found (ID: 05800001)

Default Severity	WARNING
Log Message	Virus found in file <filename>. Virus Name: <virusname>. Signature: <virussig>. Advisory ID: <advisoryid>.
Explanation	A virus has been detected in a data stream. Since anti-virus is running in protect mode, the data transfer will be aborted in order to protect the receiver.
Gateway Action	block_data
Recommended Action	If the infected file is local, run anti-virus program to clean the file.
Revision	1
Parameters	filename virusname virussig advisoryid [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.2. virus_found (ID: 05800002)

Default Severity	WARNING
Log Message	Virus found in file <filename>. Virus Name: <virusname>. Signature: <virussig>. Advisory ID: <advisoryid>.
Explanation	A virus has been detected in a data stream. Since anti-virus is running in audit mode, the data transfer will be allowed to continue.
Gateway Action	allow_data
Recommended Action	If the infected file is local, run anti-virus program to clean the file.
Revision	1
Parameters	filename virusname virussig advisoryid [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.3. excluded_file (ID: 05800003)

Default Severity	NOTICE
Log Message	File <filename> is excluded from scanning. Identified filetype: <filetype>.
Explanation	The named file will be excluded from anti-virus scanning. The filetype is present in the anti-virus scan exclusion list.
Gateway Action	allow_data_without_scan
Recommended Action	None.
Revision	1
Parameters	filename filetype [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.4. decompression_failed (ID: 05800004)

Default Severity	ERROR
Log Message	Decompression error for file <filename>
Explanation	The file could not be scanned by the anti-virus module since the decompression of the compressed file failed. Since anti-virus is running in protect mode, the data transfer will be aborted in order to protect the receiver.
Gateway Action	block_data
Recommended Action	Change Fail Mode parameter to allow if files that fail decompression should be allowed without scanning.
Revision	1
Parameters	filename [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.5. decompression_failed (ID: 05800005)

Default Severity	ERROR
Log Message	Decompression error for file <filename>

Explanation	The file could not be scanned by the anti-virus module since the decompression of the compressed file failed. Since anti-virus is running in audit mode, the data transfer will be allowed to continue.
Gateway Action	allow_data
Recommended Action	Change Fail Mode parameter to deny if files that fail decompression should be blocked.
Revision	1
Parameters	filename [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.6. compression_ratio_violation (ID: 05800006)

Default Severity	WARNING
Log Message	Compression ratio violation for file <filename>. Compression ratio threshold: <comp_ratio>
Explanation	Anti-virus has scanned a compressed file with a compression ratio higher than the specified value. Action is set to continue scan.
Gateway Action	continue_scan
Recommended Action	Files with too high compression ratio can consume large amount of resources. This can be a DOS attack.
Revision	1
Parameters	filename comp_ratio [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.7. compression_ratio_violation (ID: 05800007)

Default Severity	WARNING
Log Message	Compression ratio violation for file <filename>. Compression ratio threshold: <comp_ratio>
Explanation	Anti-virus has scanned a compressed file with a compression ratio higher than the specified value. Action is set to continue scan.
Gateway Action	abort_scan
Recommended Action	Files with too high compression ratio can consume large amount of resources. This can be a DOS attack.

Revision	1
Parameters	filename comp_ratio [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.8. compression_ratio_violation (ID: 05800008)

Default Severity	WARNING
Log Message	Compression ratio violation for file <filename>. Compression ratio threshold: <comp_ratio>
Explanation	Anti-virus has scanned a compressed file with a compression ratio higher than the specified value. Action is set to continue scan.
Gateway Action	block_data
Recommended Action	Files with too high compression ratio can consume large amount of resources. This can be a DOS attack.
Revision	1
Parameters	filename comp_ratio [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.9. out_of_memory (ID: 05800009)

Default Severity	ERROR
Log Message	Out of memory
Explanation	Memory allocation failed. Since anti-virus is running in audit mode, the data transfer will be allowed to continue.
Gateway Action	allow_data
Recommended Action	Try to free some memory by changing configuration parameters.
Revision	1
Parameters	filename filetype [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID

Connection

2.2.10. out_of_memory (ID: 05800010)

Default Severity	ERROR
Log Message	Out of memory
Explanation	Memory allocation failed. Since anti-virus is running in protect mode, the data transfer will be aborted in order to protect the receiver.
Gateway Action	block_data
Recommended Action	Try to free some memory by changing configuration parameters.
Revision	1
Parameters	filename filetype [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.11. virus_scan_failure (ID: 05800011)

Default Severity	ERROR
Log Message	Anti-virus scan engine failed for the file: <filename>
Explanation	An error occurred in the anti-virus scan engine. Since anti-virus is running in protect mode, the data transfer will be aborted in order to protect the receiver.
Gateway Action	block_data
Recommended Action	None.
Revision	1
Parameters	filename [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.12. virus_scan_failure (ID: 05800012)

Default Severity	ERROR
Log Message	Anti-virus scan engine failed for the file: <filename>
Explanation	An error occurred in the anti-virus scan engine. Since anti-virus is

	running in audit mode, the data transfer will be allowed to continue.
Gateway Action	allow_data
Recommended Action	None.
Revision	1
Parameters	filename [layer7_srcinfo] [layer7_dstinfo]
Context Parameters	ALG Module Name ALG Session ID Connection

2.2.13. failed_to_allocate_memory (ID: 05800014)

Default Severity	ERROR
Log Message	AVSE: Memory usage for virus scanning subsystem is exceeding the limit(out of memory)
Explanation	An attempt to allocate memory failed, because the subsystem is exceeding the allocated memory limit.
Gateway Action	close
Recommended Action	Try to free some of the memory used.
Revision	1

2.2.14. no_valid_license (ID: 05800015)

Default Severity	WARNING
Log Message	AVSE: Virus scanning aborted. No valid license present.
Explanation	Antivirus scanning is aborted since there is no valid license present.
Gateway Action	av_scanning_aborted
Recommended Action	If antivirus scanning is wanted, you must get a valid license with antivirus capabilities. Antivirus scanning can be turned off in order to avoid future postings of this log message.
Revision	1
Context Parameters	ALG Session ID

2.2.15. no_signature_database (ID: 05800016)

Default Severity	ERROR
Log Message	AVSE: Virus scanning aborted. No virus signatures present.
Explanation	Antivirus scanning is aborted since there is no local antivirus signature

	database.
Gateway Action	av_scanning_denied
Recommended Action	Connect your gateway to the Internet and download the antivirus database or configure automatic updates of antivirus.
Revision	1
Context Parameters	ALG Session ID

2.2.16. general_engine_error (ID: 05800017)

Default Severity	ERROR
Log Message	AVSE: Virus scanning aborted. General error occurred during initialization.
Explanation	Antivirus scanning is aborted since the scan engine returned a general error during initialization.
Gateway Action	av_scanning_aborted
Recommended Action	Try to restart the unit in order to solve this issue.
Revision	1
Context Parameters	ALG Session ID

2.2.17. out_of_memory (ID: 05800018)

Default Severity	ERROR
Log Message	AVSE: Virus scanning aborted. Out of memory during initialization.
Explanation	Antivirus scanning is aborted since the scan engine run out of memory during initialization.
Gateway Action	av_scanning_denied
Recommended Action	Review your configuration in order to free up more RAM.
Revision	1
Context Parameters	ALG Session ID

2.2.18. unknown_encoding (ID: 05800182)

Default Severity	WARNING
Log Message	SMTPALG: Content transfer encoding is unknown or not present
Explanation	Antivirus module cannot scan the attachment since the transfer encoding is missing or unknown. Fail Mode is deny so data is blocked.
Gateway Action	block_data

Recommended Action	None.
Revision	1
Parameters	filename unknown_content_transfer_encoding sender_email_address recipient_email_addresses:
Context Parameters	ALG Module Name ALG Session ID

2.2.19. unknown_encoding (ID: 05800183)

Default Severity	WARNING
Log Message	SMTPALG: Content transfer encoding is unknown or not present.
Explanation	Antivirus module cannot scan the attachment since the transfer encoding is missing or unknown. Fail Mode is allow so data is allowed without scanning.
Gateway Action	allow_data_without_scan
Recommended Action	Research the Content Transfer Encoding format.
Revision	1
Parameters	filename unknown_content_transfer_encoding sender_email_address recipient_email_addresses
Context Parameters	ALG Module Name ALG Session ID

2.3. ARP

These log messages refer to the **ARP (ARP events)** category.

2.3.1. already_exists (ID: 00300001)

Default Severity	NOTICE
Log Message	An entry for this IP address already exists
Explanation	The entry was not added as a previous entry for this IP address already exists in the ARP table.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.2. no_sender_ip (ID: 00300002)

Default Severity	NOTICE
Log Message	ARP query sender IP is 0.0.0.0
Explanation	The source IP-address of an ARP query is 0.0.0.0. Allowing.
Gateway Action	allow
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.3. no_sender_ip (ID: 00300003)

Default Severity	NOTICE
Log Message	ARP query sender IP is 0.0.0.0. Dropping
Explanation	The source IP-address of an ARP query is 0.0.0.0. Dropping packet.
Gateway Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.4. arp_response_broadcast (ID: 00300004)

Default Severity	NOTICE
Log Message	ARP response is a broadcast address
Explanation	The ARP response has a sender address which is a broadcast address. Allowing.
Gateway Action	allow
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.5. arp_response_multicast (ID: 00300005)

Default Severity	NOTICE
Log Message	ARP response is a multicast address
Explanation	The ARP response has a sender address which is a multicast address. This might be the case if there are load balancing network equipment in the network. Allowing.
Gateway Action	allow
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.6. mismatching_hwaddrs (ID: 00300006)

Default Severity	NOTICE
Log Message	ARP hw sender does not match Ethernet hw sender
Explanation	The hardware sender address specified in the ARP data does not match the Ethernet hardware sender address. Allowing.
Gateway Action	allow
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.7. mismatching_hwaddrs_drop (ID: 00300007)

Default Severity	NOTICE
Log Message	ARP hw sender does not match Ethernet hw sender. Dropping
Explanation	The hardware sender address specified in the ARP data does not match the Ethernet hardware sender address. Dropping packet.
Gateway Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.8. hwaddr_change (ID: 00300008)

Default Severity	NOTICE
Log Message	<knownip> has a different address <newhw> compared to the known hardware address <knownhw>. Allow packet for further processing.
Explanation	A known dynamic ARP entry has a different hardware address than the one in the ARP packet. Allowing packet for further processing.
Gateway Action	allow_processing
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Parameters	knownip knownhw newhw
Context Parameters	Rule Name Packet Buffer

2.3.9. arp_cache_size_limit_reached (ID: 00300030)

Default Severity	NOTICE
Log Message	ARP cache size limit reached
Explanation	The ARP cache size limit has been reached. Current license limit is [limit].
Gateway Action	None
Recommended Action	Update your license to allow a greater amount of concurrent ARP entries.
Revision	1
Parameters	limit

2.3.10. invalid_arp_sender_ip_address (ID: 00300049)

Default Severity	WARNING
Log Message	Failed to verify ARP sender IP address. Dropping
Explanation	The ARP sender IP address could not be verified according to the "access" section, and the packet is dropped.
Gateway Action	drop
Recommended Action	If all ARP sender IP addresses should be accepted without validation, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.11. arp_access_allowed_expect (ID: 00300050)

Default Severity	NOTICE
Log Message	Allowed by expect rule in access section
Explanation	The ARP sender IP address is verified by an expect rule in the access section.
Gateway Action	access_allow
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.12. impossible_hw_address (ID: 00300051)

Default Severity	NOTICE
Log Message	Impossible hardware address 0000:0000:0000 in ARP response. Dropping
Explanation	The ARP response has sender hardware address 0000:0000:0000, which is illegal. Dropping packet.
Gateway Action	drop
Recommended Action	Verify that no fault network equipment exists.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.13. arp_response_broadcast_drop (ID: 00300052)

Default Severity	WARNING
Log Message	ARP response is a broadcast address. Dropping
Explanation	The ARP response has a sender address which is a broadcast address. Dropping packet.
Gateway Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.14. arp_response_multicast_drop (ID: 00300053)

Default Severity	NOTICE
Log Message	ARP response is a multicast address. Dropping
Explanation	The ARP response has a sender address which is a multicast address. This might be the case if there are load balancing network equipment in the network. Dropping packet.
Gateway Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.3.15. arp_collides_with_static (ID: 00300054)

Default Severity	WARNING
Log Message	Known entry is <knowntype> <knownip>=<knownhw>. Dropping
Explanation	The hardware sender address does not match the static entry in the ARP table. Static ARP changes are not allowed. Dropping packet.
Gateway Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Parameters	reason knowntype knownip knownhw
Context Parameters	Rule Name Packet Buffer

2.3.16. hwaddr_change_drop (ID: 00300055)

Default Severity	NOTICE
Log Message	<knownip> has a different address <newhw> compared to the known hardware address <knownhw>. Dropping packet.
Explanation	A known dynamic ARP entry has a different hardware address than the one in the ARP packet. Dropping packet.
Gateway Action	drop
Recommended Action	If this is not the desired behaviour, modify the configuration.
Revision	1
Parameters	knownip knownhw newhw
Context Parameters	Rule Name Packet Buffer

2.4. AVUPDATE

These log messages refer to the **AVUPDATE (Antivirus Signature update)** category.

2.4.1. av_db_update_failure (ID: 05000001)

Default Severity	ALERT
Log Message	Update of the Antivirus database failed, because of <reason>
Explanation	The unit tried to update the Antivirus database, but failed. The reason for this is specified in the "reason" parameter.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.4.2. av_database_downloaded (ID: 05000002)

Default Severity	NOTICE
Log Message	New Antivirus database downloaded
Explanation	An updated version of the Antivirus database has been downloaded, which will now be used.
Gateway Action	using_new_database
Recommended Action	None.
Revision	2

2.4.3. av_db_already_up_to_date (ID: 05000003)

Default Severity	NOTICE
Log Message	Antivirus database is up-to-date
Explanation	The current Antivirus database is up-to-date, and does not need to be updated.
Gateway Action	None
Recommended Action	None.
Revision	1

2.4.4. av_db_update_denied (ID: 05000004)

Default Severity	NOTICE
-------------------------	--------

Log Message	Antivirus database could not be updated, as no valid subscription exist
Explanation	The current license does not allow the Antivirus database to be updated.
Gateway Action	None
Recommended Action	Check the system's time and/or purchase a subscription.
Revision	1

2.4.5. av_detects_invalid_system_time (ID: 05000005)

Default Severity	ERROR
Log Message	System clock is not properly set. Invalid date (<date>) in antivirus signature file. Antivirus Disabled
Explanation	The system clock is not up to date. The system clock must be set correctly in order to use the antivirus features. Antivirus features remains disabled until clock is correct and a manual antivirus update has been performed.
Gateway Action	antivirus_disabled
Recommended Action	Check and set the system time correct and perform a manual antivirus update.
Revision	1
Parameters	date

2.4.6. downloading_new_database (ID: 05000007)

Default Severity	NOTICE
Log Message	Downloading new antivirus database
Explanation	A new antivirus database is available. The database is being downloaded.
Gateway Action	downloading_new_database
Recommended Action	None.
Revision	1

2.4.7. unsynced_databases (ID: 05000008)

Default Severity	WARNING
Log Message	Unsynchronized hardware and software databases detected
Explanation	The anti-virus hardware and software databases are not synchronized. A full update is automatically initiated.
Gateway Action	downloading_new_database

Recommended Action	None.
Revision	1

2.5. BLACKLIST

These log messages refer to the **BLACKLIST (Blacklist events)** category.

2.5.1. failed_to_write_list_of_blocked_hosts_to_media (ID: 04600001)

Default Severity	CRITICAL
Log Message	Failed to write list of blocked hosts to media
Explanation	Failed to write list of blocked hosts to media. The media might be corrupted.
Gateway Action	none
Recommended Action	Verify that the media is intact.
Revision	1

2.5.2. unable_to_allocate_static_entry (ID: 04600002)

Default Severity	WARNING
Log Message	Unable to allocate static entry for <host>
Explanation	Unable to allocate static entry. Unit is low on memory.
Gateway Action	no_block
Recommended Action	Review the configuration in order to free more RAM.
Revision	1
Parameters	host

2.5.3. unable_to_allocate_host_entry (ID: 04600003)

Default Severity	WARNING
Log Message	Unable to allocate dynamic entry for <host>
Explanation	Unable to allocate dynamic entry. Unit is low on memory.
Gateway Action	no_block
Recommended Action	Review the configuration in order to free more RAM.
Revision	1
Parameters	host

2.5.4. connection_blacklisted (ID: 04600004)

Default Severity	NOTICE
Log Message	Found <blacklisted_host> in blacklist. Triggered rule <rule>, description: <description>. Protocol: <proto>, IP: <ip>, Port: <port>.
Explanation	A blacklist entry was added which matched the IP address of this connection. Thus it was closed accordingly.
Gateway Action	close
Recommended Action	Investigate threshold or IntrusionDetection rules that could have triggered dynamic blacklisting.
Revision	1
Parameters	blacklisted_host rule description ip proto port

2.5.5. packet_blacklisted (ID: 04600005)

Default Severity	NOTICE
Log Message	Found <blacklisted_host> in blacklist. Triggered rule <rule>, description: <description>. Protocol: <proto>, IP: <ip>, Port: <port>.
Explanation	A blacklist entry was added which matched the IP address of this packet. Thus it was dropped accordingly.
Gateway Action	drop
Recommended Action	Investigate threshold or IntrusionDetection rules that could have triggered dynamic blacklisting.
Revision	1
Parameters	blacklisted_host rule description ip proto port

2.5.6. packet_blacklisted (ID: 04600006)

Default Severity	NOTICE
Log Message	Found source in blacklist. Triggered rule <rule>, description: <description>. Protocol: <proto>, IP: <ip>, Port: <port>.
Explanation	A blacklist entry was added which matched the IP address of this packet. Thus it was dropped accordingly.
Gateway Action	drop
Recommended Action	Investigate threshold or IntrusionDetection rules that could have

triggered dynamic blacklisting.

Revision

1

Parameters

rule
description
proto
ip
port

2.6. BUFFERS

These log messages refer to the **BUFFERS (Events regarding buffer usage)** category.

2.6.1. buffers_flooded (ID: 00500001)

Default Severity	WARNING
Log Message	The buffers were flooded for <duration> seconds. Current usage is <buf_usage> percent
Explanation	The unit was temporarily out of buffers for a period of time. This could be a result of a period of heavy network traffic load.
Gateway Action	None
Recommended Action	If this is a reoccurring event, try increasing the number of buffers.
Revision	1
Parameters	duration buf_usage

2.7. CONN

These log messages refer to the **CONN (State engine events, e.g. open/close connections)** category.

2.7.1. conn_open (ID: 00600001)

Default Severity	INFORMATIONAL
Log Message	Connection opened
Explanation	A connection has been opened.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	Rule Information Connection Packet Buffer

2.7.2. conn_close (ID: 00600002)

Default Severity	INFORMATIONAL
Log Message	Connection closed
Explanation	A connection has been closed.
Gateway Action	close
Recommended Action	None.
Revision	1
Context Parameters	Rule Information Connection

2.7.3. connection_table_full (ID: 00600003)

Default Severity	WARNING
Log Message	Closing (replacing) this connection; connection table full
Explanation	The connection table is currently full, and the unit needs to open a new connection. This specific connection is closed, and replaced with the new connection.
Gateway Action	replacing_conn
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

Connection

2.7.4. out_of_connections (ID: 00600010)

Default Severity	WARNING
Log Message	Out of connections. Rejecting connection attempt
Explanation	The connection table is currently full, and this new connection attempt will be rejected.
Gateway Action	reject
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.7.5. out_of_connections (ID: 00600011)

Default Severity	WARNING
Log Message	Out of connections. Dropping connection attempt
Explanation	The connection table is currently full, and this new connection attempt will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.7.6. no_new_conn_for_this_packet (ID: 00600012)

Default Severity	WARNING
Log Message	State inspector would not open a new connection for this TCP packet, rejecting
Explanation	State inspector would not open a new connection for this TCP packet since the combination of TCP flags is wrong. Only packets with the SYN TCP-flag set as the only TCP flag are allowed to open a new TCP connection.
Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	protocol

Context Parameters	Rule Name Packet Buffer
---------------------------	----------------------------

2.7.7. no_new_conn_for_this_packet (ID: 00600013)

Default Severity	WARNING
Log Message	State inspector would not open a new connection for this ICMP packet, dropping packet
Explanation	State inspector would not open a new connection for this ICMP packet since it is not an ICMP Echo Request. Only Echo Requests are allowed to open a new ICMP connection.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	protocol
Context Parameters	Rule Name Packet Buffer

2.7.8. no_return_route (ID: 00600014)

Default Severity	WARNING
Log Message	Failed to open a new connection since a return route to the sender address cant be found. Dropping packet
Explanation	There was no return route found to the sender address of the packet. Therefore, a new connection could not be opened and the packet is dropped.
Gateway Action	reject
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Connection Packet Buffer

2.7.9. reverse_connect_attempt (ID: 00600015)

Default Severity	WARNING
Log Message	Disallowed reverse connect attempt from peer. Dropping
Explanation	State inspector does not allow this packet in reverse direction on the already opened connection. This type of packet is only allowed to be sent by the originator of a connection. Dropping the packet.
Gateway Action	drop

Recommended Action	None.
Revision	1
Context Parameters	Rule Name Connection Packet Buffer

2.7.10. port_0_illegal (ID: 00600020)

Default Severity	WARNING
Log Message	TCP/UDP destination port or TCP source port was set to 0. Dropping
Explanation	The TCP/UDP destination or TCP source port was set to 0, which is not allowed. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.7.11. udp_src_port_0_illegal (ID: 00600021)

Default Severity	WARNING
Log Message	UDP source port is set to 0. Dropping
Explanation	The UDP source port was set to 0. This can be used by UDP streams not expecting return traffic. Dropping packet.
Gateway Action	drop
Recommended Action	If the packet is wanted, change the UDP source port 0 setting.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.7.12. udp_src_port_0_forwarded (ID: 00600022)

Default Severity	WARNING
Log Message	UDP source port is set to 0. Forwards packet
Explanation	The UDP source port was set to 0. This can be used by UDP streams not expecting return traffic. Forwarding packet.
Gateway Action	none
Recommended Action	None.

Revision	1
Context Parameters	Rule Name Packet Buffer

2.7.13. conn_usage (ID: 00600023)

Default Severity	INFORMATIONAL
Log Message	Connection used to forward a packet.
Explanation	A packet has passed through the connection.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	Packet Buffer

2.7.14. active_data (ID: 00600100)

Default Severity	INFORMATIONAL
Log Message	FTPALG: Incoming active data channel
Explanation	An active data channel connection has been established.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID Rule Information Connection

2.7.15. passive_data (ID: 00600101)

Default Severity	INFORMATIONAL
Log Message	FTPALG: Incoming passive data channel
Explanation	A passive data channel connection has been established.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID Rule Information

Connection

2.7.16. active_data (ID: 00600102)

Default Severity	INFORMATIONAL
Log Message	FTPALG: Active data channel closed
Explanation	An active data channel was closed.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID Rule Information Connection

2.7.17. passive_data (ID: 00600103)

Default Severity	INFORMATIONAL
Log Message	FTPALG: Passive data channel closed
Explanation	A passive data channel was closed.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	ALG Module Name ALG Session ID Rule Information Connection

2.8. DEVICEMONITOR

These log messages refer to the **DEVICEMONITOR (Device monitor events)** category.



Note

The log message IDs in this category are assigned dynamically based on the device monitor configuration. The variable part of the ID (indicated by *x* below) corresponds to the assigned ID of the device monitor rule that triggered, e.g. assigned ID 1 results in log message ID 05400001 and assigned ID 12 becomes log message ID 05400012.

2.8.1. value_above_high_threshold (ID: 054xxxxx)

Default Severity	INFORMATIONAL
Log Message	Security Gateway Monitoring. Current uptime: <uptime>. The value of: <name> is above the high threshold High threshold: <threshold> Current mean of <numbersamples>: <currentvalue>.
Explanation	High threshold passed.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	uptime name threshold numbersamples currentvalue

2.8.2. value_below_low_threshold (ID: 054xxxxx)

Default Severity	INFORMATIONAL
Log Message	Security Gateway Monitoring. Current uptime: <uptime>. The value of: <name> is below the low threshold Low threshold: <threshold> Current mean of <numbersamples>: <currentvalue>.
Explanation	Low threshold passed.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	uptime name threshold numbersamples currentvalue

2.8.3. value_below_high_threshold (ID: 054xxxxx)

Default Severity	INFORMATIONAL
Log Message	Security Gateway Monitoring. Current uptime: <uptime>. The value of: <name> is now bellow the high threshold Low threshold: <threshold> Current mean of <numbersamples>: <currentvalue>.
Explanation	Low threshold passed.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	uptime name threshold numbersamples currentvalue

2.8.4. value_above_low_threshold (ID: 054xxxxx)

Default Severity	INFORMATIONAL
Log Message	Security Gateway Monitoring. Current uptime: <uptime>. The value of: <name> is above the low threshold Low threshold: <threshold> Current mean of <numbersamples>: <currentvalue>.
Explanation	Low threshold passed.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	uptime name threshold numbersamples currentvalue

2.9. DHCP

These log messages refer to the **DHCP (DHCP client events)** category.

2.9.1. offered_ip_occupied (ID: 00700001)

Default Severity	NOTICE
Log Message	Interface <iface> received a lease with an offered IP that appear to be occupied (<ip4addr>)
Explanation	Received a DHCP lease which appears to be in use by someone else.
Gateway Action	restart
Recommended Action	Check network for statically configured hosts or incorrectly proxy ARPed routes.
Revision	1
Parameters	iface ip4addr

2.9.2. lease_changed (ID: 00700002)

Default Severity	WARNING
Log Message	Some vital parameter(s) in the lease on interface <iface> have changed, restarting DHCP-process
Explanation	The DHCP server have updated some information considered vital. This will result in the DHCP process being restarted.
Gateway Action	restart
Recommended Action	None.
Revision	1
Parameters	iface
Context Parameters	Packet Buffer

2.9.3. lease_acquired (ID: 00700003)

Default Severity	NOTICE
Log Message	Interface <iface> have successfully acquired a lease
Explanation	An interface have successfully acquired a lease.
Gateway Action	None
Recommended Action	None.
Revision	1

Parameters	iface ip netmask bcast gw
Context Parameters	Packet Buffer

2.9.4. renewed_lease (ID: 00700004)

Default Severity	NOTICE
Log Message	Interface <iface> have renewed its lease. The new lease is valid for <valid_seconds> seconds
Explanation	An interface have successfully renewed its lease.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface valid_seconds
Context Parameters	Packet Buffer

2.9.5. lease_expired (ID: 00700005)

Default Severity	NOTICE
Log Message	Interface <iface> lease expired
Explanation	A lease have expired and the ip data for this interface are no longer valid.
Gateway Action	restart
Recommended Action	Check connection and DHCP server reachability.
Revision	1
Parameters	iface

2.9.6. invalid_lease_time (ID: 00700007)

Default Severity	WARNING
Log Message	Interface <iface> received a lease with a leasetime (<lease_time>) which is lower then the minimum allowed (<minimum_lease_time>)
Explanation	An interface received a lease with a leasetime which is lower then the configured minimum.
Gateway Action	drop

Recommended Action	Check the DHCP server configuration or adjust the minimum leasetime limit.
Revision	1
Parameters	iface lease_time minimum_lease_time
Context Parameters	Packet Buffer

2.9.7. invalid_server_id (ID: 00700008)

Default Severity	WARNING
Log Message	Interface <iface> received a lease with an invalid server ID (<server_id>)
Explanation	An interface received a lease with an invalid server ID parameter.
Gateway Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface server_id
Context Parameters	Packet Buffer

2.9.8. invalid_netmask (ID: 00700009)

Default Severity	WARNING
Log Message	Interface <iface> received a lease with an invalid netmask (<netmask>)
Explanation	An interface received a lease with an invalid netmask.
Gateway Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface netmask
Context Parameters	Packet Buffer

2.9.9. invalid_broadcast (ID: 00700010)

Default Severity	WARNING
Log Message	Interface <iface> received a lease with an invalid broadcast address (<broadcast>)

Explanation	An interface received a lease with an invalid broadcast address.
Gateway Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface broadcast
Context Parameters	Packet Buffer

2.9.10. invalid_offered_ip (ID: 00700011)

Default Severity	WARNING
Log Message	Interface <iface> received a lease with an invalid offered IP (<offered_ip>)
Explanation	An interface received a lease with an invalid offered IP address.
Gateway Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface offered_ip
Context Parameters	Packet Buffer

2.9.11. invalid_gateway (ID: 00700012)

Default Severity	WARNING
Log Message	Interface <iface> received a lease with an invalid gateway (<gateway>)
Explanation	An interface received a lease with an invalid gateway address.
Gateway Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface gateway
Context Parameters	Packet Buffer

2.9.12. offered_broadcast_equals_gateway (ID: 00700013)

Default Severity	WARNING
-------------------------	---------

Log Message	Interface <iface> received a lease where the offered broadcast equals the offered gateway
Explanation	An interface received a lease where the offered broadcast address is equal with the offered gateway address.
Gateway Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	iface
Context Parameters	Packet Buffer

2.9.13. ip_collision (ID: 00700014)

Default Severity	WARNING
Log Message	Interface <iface> received a lease which if used will cause an IP collision (DHCP IP: <dhcp_ip> collides with configured route: <configured_route>)
Explanation	An interface received a lease which if used will cause an IP collision with a configured route.
Gateway Action	drop
Recommended Action	Check DHCP server configuration and the SG interface configuration.
Revision	1
Parameters	iface dhcp_ip configured_route
Context Parameters	Packet Buffer

2.9.14. route_collision (ID: 00700015)

Default Severity	WARNING
Log Message	Interface <iface> received a lease which if used will cause a route collision (DHCP route: <dhcp_route> collides with configured route <configured_route>)
Explanation	An interface received a lease which if used will cause a route collision with a configured route.
Gateway Action	drop
Recommended Action	Check DHCP server configuration and SG interface configuration.
Revision	1
Parameters	iface dhcp_route configured_route

Context Parameters

Packet Buffer

2.10. DHCPRELAY

These log messages refer to the **DHCPRELAY (DHCP relay events)** category.

2.10.1. unable_to_save_dhcp_relay_list (ID: 00800001)

Default Severity	WARNING
Log Message	Unable to auto save the DHCP relay list to disk
Explanation	Unable to autosave the DHCP relay list to disk.
Gateway Action	None
Recommended Action	Check disk usage and health.
Revision	1

2.10.2. dhcp_relay_list_saved (ID: 00800002)

Default Severity	NOTICE
Log Message	DHCP relay list was successfully auto saved to disk
Explanation	The DHCP relay list was successfully written to disk.
Gateway Action	None
Recommended Action	None.
Revision	1

2.10.3. dhcp_pkt_too_small (ID: 00800003)

Default Severity	NOTICE
Log Message	Received DHCP packet which is smaller then the minimum allowed 300 bytes.
Explanation	Received a DHCP packet which is smaller then the minimum allowed 300 bytes.
Gateway Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Packet Buffer

2.10.4. incorrect_bootp_dhcp_cookie (ID: 00800004)

Default Severity	WARNING
-------------------------	---------

Log Message	Incorrect BOOTP/DHCP cookie. Dropping
Explanation	Received a packet with an incorrect BOOTP/DHCP cookie.
Gateway Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Packet Buffer

2.10.5. maximum_ppm_for_relayer_reached (ID: 00800005)

Default Severity	WARNING
Log Message	The maximum packets-per-minute limit have been reached. Requests will be denied for a period of time
Explanation	The maximum DHCP packets-per-minute limit for the relayer have been reached.
Gateway Action	None
Recommended Action	Verify packets-per-minute limit.
Revision	1
Context Parameters	Packet Buffer

2.10.6. relayer_resuming (ID: 00800006)

Default Severity	NOTICE
Log Message	The relayer is now resuming, <packets_dropped> packets were dropped while the relayer was inactive
Explanation	The relayer is now resuming its duties since being temporary halted by the packets-per-minute limit.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	packets_dropped
Context Parameters	Packet Buffer

2.10.7. hop_limit_exceeded (ID: 00800007)

Default Severity	WARNING
Log Message	Hop limit exceeded. Dropping
Explanation	The maximum hop limit for the DHCP packet have been reached.

Gateway Action	None
Recommended Action	Verify maximum-hop-limit setting.
Revision	1
Context Parameters	Packet Buffer

2.10.8. client_release (ID: 00800008)

Default Severity	WARNING
Log Message	Client <client_ip> requested release. Relay canceled
Explanation	A client requested that lease should be canceled.
Gateway Action	relay_canceled
Recommended Action	None.
Revision	1
Parameters	client_ip
Context Parameters	Packet Buffer

2.10.9. got_reply_without_transaction_state (ID: 00800009)

Default Severity	WARNING
Log Message	Got server reply without transaction state for client <client_hw>. Dropping
Explanation	Received a server reply without a matching transaction state.
Gateway Action	drop
Recommended Action	Check the network environment for errors.
Revision	1
Parameters	client_hw
Context Parameters	Packet Buffer

2.10.10. maximum_dhcp_client_relay_routes_reached (ID: 00800010)

Default Severity	WARNING
Log Message	The limit for DHCP relay routes have been reached. Dropping
Explanation	The DHCP relay routes limit have been reached.
Gateway Action	drop

Recommended Action	Verify max-relay-routes-limit.
Revision	1
Context Parameters	Rule Name

2.10.11. unable_to_add_relay_route_since_out_of_memory (ID: 00800011)

Default Severity	ERROR
Log Message	Internal Error: Out of memory: Can't add DHCP relay route. Dropping
Explanation	Unable to add DHCP relay route since out of memory.
Gateway Action	drop
Recommended Action	Check firewall memory consumption.
Revision	1
Context Parameters	Rule Name

2.10.12. ignored_relay_request (ID: 00800012)

Default Severity	WARNING
Log Message	Request ignored according to the ruleset
Explanation	A DHCP relay request was ignored according to the rules.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.13. no_message_type (ID: 00800013)

Default Severity	WARNING
Log Message	No message type. Dropping
Explanation	Received DHCP packet without the required message type parameter.
Gateway Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.14. bad_inform_pkt_with_mismatching_source_ip_and_client_ip (ID: 00800014)

Default Severity	WARNING
Log Message	INFORM packet did not pass through a relay but the packet source ip and the client ip doesnt match. Dropping
Explanation	Received non relayed INFORM DHCP packet with illegally mismatching source and client IP.
Gateway Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.15. received_relayed_inform_packet_without_client_ip (ID: 00800015)

Default Severity	WARNING
Log Message	INFORM packet passed a relay but the client ip isnt set. Dropping
Explanation	Received relayed INFORM DHCP packet with illegally missing client IP.
Gateway Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.10.16. maximum_current_dhcp_relays_for_iface (ID: 00800016)

Default Severity	WARNING
Log Message	The maximum number <max_relays> of current DHCP relays for this interface have been reached. Dropping
Explanation	The maximum number of DHCP relayed through a specified interface have been reached.
Gateway Action	drop
Recommended Action	Verify max-relay-per-interface setting.
Revision	1

Parameters	max_relays
Context Parameters	Rule Name Packet Buffer

2.10.17. dhcp_server_is_unroutable (ID: 00800017)

Default Severity	WARNING
Log Message	BOOTP/DHCP-server at <dest_ip> is unroutable. Dropping
Explanation	Unable to find route to specified DHCP server.
Gateway Action	drop
Recommended Action	Update routing table with a route to the DHCP server.
Revision	1
Parameters	dest_ip
Context Parameters	Rule Name Packet Buffer

2.10.18. unable_to_get_free_transaction_state (ID: 00800018)

Default Severity	WARNING
Log Message	Unable to get free transaction state for client <client_hw>. Dropping
Explanation	Unable to get a free transaction state to handle client request.
Gateway Action	drop
Recommended Action	Verify max-transaction-count setting.
Revision	1
Parameters	client_hw
Context Parameters	Rule Name Packet Buffer

2.10.19. invalid_gateway (ID: 00800019)

Default Severity	WARNING
Log Message	Received request with invalid gateway (<gateway_ip>). Dropping
Explanation	Received DHCP request with an invalid gateway.
Gateway Action	drop
Recommended Action	Investigate what client implementation is being used.

Revision	1
Parameters	gateway_ip
Context Parameters	Rule Name Packet Buffer

2.10.20. relayed_request (ID: 00800020)

Default Severity	NOTICE
Log Message	Relayed DHCP-request <type> from client <client_hw> to <dest_ip>
Explanation	Relayed a DHCP request.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	type client_hw dest_ip
Context Parameters	Rule Name Packet Buffer

2.10.21. relayed_request (ID: 00800021)

Default Severity	NOTICE
Log Message	Relayed BOOTP-request from client <client_hw> to <dest_ip>
Explanation	Relayed a BOOTP request.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	client_hw dest_ip
Context Parameters	Rule Name Packet Buffer

2.10.22. got_reply_on_a_non_security_equivalent_interface (ID: 00800022)

Default Severity	WARNING
Log Message	Received reply for client <client_hw> on a non security equivalent interface. Dropping

Explanation	Received a reply for a client on a non security equivalent interface.
Gateway Action	drop
Recommended Action	Verify security-equivalent-interface setting.
Revision	1
Parameters	client_hw
Context Parameters	Rule Name Packet Buffer

2.10.23. assigned_ip_not_allowed (ID: 00800023)

Default Severity	WARNING
Log Message	DHCP/BOOTP-Server <server_ip> gave out an IP <ip> which isn't accepted. Dropping
Explanation	Received a lease with an IP which is not accepted according to the rules.
Gateway Action	drop
Recommended Action	Verify allowed-lease-addresses setting.
Revision	1
Parameters	iface server_ip ip
Context Parameters	Rule Name Packet Buffer

2.10.24. illegal_client_ip_assignment (ID: 00800024)

Default Severity	WARNING
Log Message	DHCP/BOOTP-Server <server_ip> tried to assign a client with an illegal IP <ip>. Dropping
Explanation	Received a lease with an illegal client assignment IP.
Gateway Action	drop
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	server_ip ip
Context Parameters	Rule Name Packet Buffer

2.10.25. ambiguous_host_route (ID: 00800025)

Default Severity	WARNING
Log Message	A host route for <dest_ip> already exists which points to another interface. Dropping
Explanation	An ambiguous host route indicating another interface was detected trying to setup a dynamic hostroute for a client.
Gateway Action	drop
Recommended Action	Review previous configured host route for client.
Revision	1
Parameters	dest_ip
Context Parameters	Rule Name Packet Buffer

2.10.26. relayed_dhcp_reply (ID: 00800026)

Default Severity	NOTICE
Log Message	Relayed DHCP-reply <type> to client <client_hw>
Explanation	Relayed DHCP reply to client.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	type client_hw
Context Parameters	Rule Name Packet Buffer

2.10.27. relayed_bootp_reply (ID: 00800027)

Default Severity	NOTICE
Log Message	Relayed BOOTP-reply to client <client_hw>
Explanation	Relayed BOOTP reply to client.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	client_hw
Context Parameters	Rule Name Packet Buffer

2.10.28. relayed_dhcp_reply (ID: 00800028)

Default Severity	NOTICE
Log Message	Relayed DHCP-reply <type> to gateway <gateway_ip>
Explanation	Relayed DHCP reply to a gateway.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	type gateway_ip
Context Parameters	Rule Name Packet Buffer

2.10.29. relayed_bootp_reply (ID: 00800029)

Default Severity	NOTICE
Log Message	Relayed BOOTP-reply to gateway <gateway_ip>
Explanation	Relayed BOOTP reply to a gateway.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	gateway_ip
Context Parameters	Rule Name Packet Buffer

2.11. DHCPSEVER

These log messages refer to the **DHCPSEVER (DHCP server events)** category.

2.11.1. unable_to_send_response (ID: 00900001)

Default Severity	WARNING
Log Message	Failed to get buffer for sending. Unable to reply
Explanation	Unable to get a buffer for sending.
Gateway Action	None
Recommended Action	Check buffer consumption.
Revision	1

2.11.2. option_section_is_too_big_unable_to_reply (ID: 00900002)

Default Severity	WARNING
Log Message	The option section is too big, unable to reply. Dropping
Explanation	Unable to send reply since the DHCP option section is too big.
Gateway Action	drop
Recommended Action	Reduce the number of used DHCP options.
Revision	1

2.11.3. unable_to_save_lease_db (ID: 00900003)

Default Severity	WARNING
Log Message	Unable to auto save the lease database to disk
Explanation	Some sort of error occurred saving the lease database to disk.
Gateway Action	None
Recommended Action	Make sure that there is sufficient disk space available.
Revision	1

2.11.4. lease_db_successfully_saved (ID: 00900004)

Default Severity	NOTICE
Log Message	Lease database was successfully auto saved to disk
Explanation	The lease database was successfully saved to disk.

Gateway Action	None
Recommended Action	None.
Revision	1

2.11.5. dhcp_packet_too_small (ID: 00900005)

Default Severity	WARNING
Log Message	Received DHCP packet which is smaller then the minimum allowed 300 bytes. Dropping
Explanation	Received a DHCP packet which is smaller then the minimum allowed 300 bytes.
Gateway Action	drop
Recommended Action	Investigate what client implementation is being used.
Revision	1
Context Parameters	Packet Buffer

2.11.6. request_for_ip_from_non_bound_client_without_state (ID: 00900006)

Default Severity	WARNING
Log Message	Received a request from client(not in bound) <client> for IP <client_ip> without state. Rejecting
Explanation	Received a request from a non bound client without state.
Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	client client_ip
Context Parameters	Packet Buffer

2.11.7. request_for_ip_from_bound_client_without_state (ID: 00900007)

Default Severity	WARNING
Log Message	Received a request from client(in bound) <client> for IP <client_ip> without state. Rejecting
Explanation	Received a request from a bound client without state.

Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	client client_ip
Context Parameters	Packet Buffer

2.11.8. request_for_ip_from_non_bound_client_without_state (ID: 00900008)

Default Severity	WARNING
Log Message	Received a request from client(not in bound) <client> for IP <client_ip> without state. Ignoring
Explanation	Received a request from an unbound client without state.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	client client_ip
Context Parameters	Packet Buffer

2.11.9. all_ip_pools_depleted (ID: 00900010)

Default Severity	WARNING
Log Message	All IP pools are depleted. Unable to handle request. Ignoring
Explanation	All IP pools have been depleted.
Gateway Action	None
Recommended Action	Extend the pools to support more clients.
Revision	1
Context Parameters	Packet Buffer

2.11.10. request_with_bad_udp_checksum (ID: 00900011)

Default Severity	WARNING
Log Message	Received request with bad UDP checksum. Dropping
Explanation	Received request with bad UDP checksum.

Gateway Action	drop
Recommended Action	Check network equipment for errors.
Revision	1
Context Parameters	Packet Buffer

2.11.11. lease_timeout (ID: 00900012)

Default Severity	NOTICE
Log Message	Lease for IP <client_ip> timed out. Was bound to client <client_hw>
Explanation	A client lease wasn't renewed and timed out.
Gateway Action	lease_inactive
Recommended Action	None.
Revision	1
Parameters	client_ip client_hw
Context Parameters	Rule Name

2.11.12. lease_timeout (ID: 00900013)

Default Severity	NOTICE
Log Message	Offer for IP <client_ip> timed out. Was offered to client <client_hw>
Explanation	An offer to a client was never accepted and timed out.
Gateway Action	lease_inactive
Recommended Action	None.
Revision	1
Parameters	client_ip client_hw
Context Parameters	Rule Name

2.11.13. pool_depleted (ID: 00900014)

Default Severity	WARNING
Log Message	All IPs in the pool are in use. Request cannot be fulfilled
Explanation	A request cannot be fulfilled since all pools are in use.
Gateway Action	None
Recommended Action	Extend the pools to support more clients.

Revision	1
Context Parameters	Rule Name Packet Buffer

2.11.14. sending_offer (ID: 00900015)

Default Severity	NOTICE
Log Message	Received DISCOVER from client <client_hw>. Sending IP offer <offer_ip>
Explanation	Received discover (initial IP query) from a client.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	client_hw offer_ip
Context Parameters	Rule Name Packet Buffer

2.11.15. pool_depleted (ID: 00900016)

Default Severity	NOTICE
Log Message	All IPs in the pool are now in use
Explanation	All IPs the the pool have been consumed.
Gateway Action	None
Recommended Action	Extend the pool to support more clients.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.11.16. request_for_non_offered_ip (ID: 00900017)

Default Severity	WARNING
Log Message	Client <client_hw> requested non offered IP. Rejecting
Explanation	Client sent a request for a non offered IP.
Gateway Action	nak
Recommended Action	None.
Revision	1

Parameters	client_hw client_wanted client_offered
Context Parameters	Rule Name Packet Buffer

2.11.17. request_for_non_bound_ip (ID: 00900018)

Default Severity	WARNING
Log Message	Client <client_hw> requested non bound IP. Rejecting
Explanation	Client requested a non bound IP.
Gateway Action	reject
Recommended Action	None.
Revision	1
Parameters	client_hw client_wanted bound
Context Parameters	Rule Name Packet Buffer

2.11.18. client_bound (ID: 00900019)

Default Severity	NOTICE
Log Message	Client <client_hw> accepted IP <client_ip>. Client is now bound
Explanation	Client accepted the IP address and are now bound.
Gateway Action	new_lease
Recommended Action	None.
Revision	1
Parameters	client_hw client_ip
Context Parameters	Rule Name Packet Buffer

2.11.19. client_renewed (ID: 00900020)

Default Severity	NOTICE
Log Message	Client <client_hw> renewed IP <client_ip>
Explanation	Client successfully renewed its lease.
Gateway Action	renew

Recommended Action	None.
Revision	1
Parameters	client_hw client_ip
Context Parameters	Rule Name Packet Buffer

2.11.20. got_inform_request (ID: 00900021)

Default Severity	NOTICE
Log Message	Got INFORM request from client <client_hw>. Acknowledging
Explanation	Got an inform (client already got an IP and asks for configuration parameters) request from a client.
Gateway Action	acknowledging
Recommended Action	None.
Revision	1
Parameters	client_hw client_ip
Context Parameters	Rule Name Packet Buffer

2.11.21. decline_for_ip_on_wrong_iface (ID: 00900022)

Default Severity	NOTICE
Log Message	Got decline for ip <client_ip> on wrong interface (recv: <recv_if>, lease: <client_if>). Decline is ignored
Explanation	Got decline from a client on the wrong interface.
Gateway Action	None
Recommended Action	Check network for inconsistent routes.
Revision	1
Parameters	client_hw client_ip recv_if client_if
Context Parameters	Rule Name Packet Buffer

2.11.22. decline_for_non_offered_ip (ID: 00900023)

Default Severity	NOTICE
-------------------------	--------

Log Message	Client <client_hw> declined non offered IP. Decline is ignored
Explanation	Client rejected non a offered IP.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	client_hw
Context Parameters	Rule Name Packet Buffer

2.11.23. declined_by_client (ID: 00900024)

Default Severity	WARNING
Log Message	Client <client_hw> declined IP <client_ip>. IP blacklisted
Explanation	A client declined (indicated that the IP is already in use someone else) offered IP.
Gateway Action	blacklist
Recommended Action	Check network for statically configured hosts or incorrectly proxy ARPed routes.
Revision	1
Parameters	client_hw client_ip
Context Parameters	Rule Name Packet Buffer

2.11.24. request_for_ip_from_bound_client_without_state (ID: 00900025)

Default Severity	WARNING
Log Message	Received a request from client(bound) <client> for IP <client_ip> without state. Ignoring
Explanation	Received a request from a bound client without state.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	client client_ip
Context Parameters	Packet Buffer

2.11.25. release_for_ip_on_wrong_iface (ID: 00900026)

Default Severity	WARNING
Log Message	Got release for ip <client_ip> on wrong interface (recv: <recv_if>, lease: <client_if>). Decline is ignored
Explanation	Got release from a client on the wrong interface.
Gateway Action	None
Recommended Action	Check network for inconsistent routes.
Revision	1
Parameters	client_hw client_ip recv_if client_if
Context Parameters	Rule Name Packet Buffer

2.11.26. released_by_client (ID: 00900027)

Default Severity	NOTICE
Log Message	Client <client_hw> released IP <client_ip>.
Explanation	A client released (prematurely ended) its lease.
Gateway Action	lease_released
Recommended Action	None.
Revision	1
Parameters	client_hw client_ip
Context Parameters	Rule Name Packet Buffer

2.12. DYNROUTING

These log messages refer to the **DYNROUTING (Dynamic routing)** category.

2.12.1. failed_to_export_route_to_ospf_process_failed_to_alloc (ID: 01100001)

Default Severity	CRITICAL
Log Message	Failed to export route to OSPF process (unable to alloc export node)
Explanation	Unable to export route to a OSPF process since out of memory.
Gateway Action	alert
Recommended Action	Check memory consumption.
Revision	1
Context Parameters	Dynamic Route Rule Name Route

2.12.2. route_exported_to_ospf_as (ID: 01100002)

Default Severity	NOTICE
Log Message	Route exported to OSPF AS
Explanation	A route was just exported to a OSPF AS.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	Dynamic Route Rule Name Route

2.12.3. route_unexported_from_ospf_as (ID: 01100003)

Default Severity	NOTICE
Log Message	Route unexported from OSPF AS
Explanation	A route was just unexported from a OSPF AS.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	Dynamic Route

Rule Name
Route

2.12.4. failed_to_add_route_unable_to_alloc (ID: 01100004)

Default Severity	CRITICAL
Log Message	Failed to add route (unable to alloc route)
Explanation	Failed to create a route since out of memory.
Gateway Action	alert
Recommended Action	Check memory consumption.
Revision	1
Context Parameters	Dynamic Route Rule Name Route

2.12.5. route_added (ID: 01100005)

Default Severity	NOTICE
Log Message	Route added
Explanation	A route was just added.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	Dynamic Route Rule Name Route

2.12.6. route_removed (ID: 01100006)

Default Severity	NOTICE
Log Message	Route removed
Explanation	A route was just removed.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	Dynamic Route Rule Name Route

2.13. FRAG

These log messages refer to the **FRAG (Fragmentation events)** category.

2.13.1. individual_frag_timeout (ID: 02000001)

Default Severity	WARNING
Log Message	Individual fragment timed out.
Explanation	A fragment of an IP packet timed out, and is dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.2. fragact_contains_frags (ID: 02000002)

Default Severity	CRITICAL
Log Message	Internal Error: A failed active fragment contained fragments. Dropping
Explanation	An Internal Error occurred when freeing an active fragment. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Dropped Fragments Rule Name

2.13.3. fail_suspect_out_of_resources (ID: 02000003)

Default Severity	CRITICAL
Log Message	Out of reassembly resources for suspect. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	Out of fragmentation-reassembly resources when processing the IP packet, which may contain illegal fragments. Dropping packet and freeing resources.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip

	destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.13.4. fail_out_of_resources (ID: 02000004)

Default Severity	CRITICAL
Log Message	Out of reassembly resources. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	Out of fragmentation-reassembly resources when processing the IP packet. Dropping packet and freeing resources.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.13.5. fail_suspect_timeout (ID: 02000005)

Default Severity	CRITICAL
Log Message	Time out reassembling suspect. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	Timed out when reassembling a fragmented IP packet, which may contain illegal fragments. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments

Rule Name

2.13.6. fail_timeout (ID: 02000006)

Default Severity	CRITICAL
Log Message	Time out reassembling. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	Timed out when reassembling a fragmented IP packet. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.13.7. disallowed_suspect (ID: 02000007)

Default Severity	WARNING
Log Message	Dropping stored fragments of disallowed suspect packet. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	The fragments of a disallowed IP packet, which may contain illegal fragments, were dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.13.8. drop_frags_of_disallowed_packet (ID: 02000008)

Default Severity	WARNING
Log Message	Dropping stored fragments of disallowed packet. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	The fragments of a disallowed IP packet were dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.13.9. drop_frags_of_illegal_packet (ID: 02000009)

Default Severity	WARNING
Log Message	Dropping fragments of illegal packet. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	The fragments of an illegal IP packet were dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.13.10. drop_extraneous_frags_of_completed_packet (ID: 02000010)

Default Severity	WARNING
Log Message	Dropping extraneous fragments of completed packet. Frags: <frags>. <srcip>-<destip> <ipproto> FragID: <fragid>, State: <fragact>
Explanation	A completed reassembled IP packet contains extraneous fragments,

	which are dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	srcip destip ipproto fragid fragact frags
Context Parameters	Dropped Fragments Rule Name

2.13.11. learn_state (ID: 02000011)

Default Severity	ERROR
Log Message	Internal Error: Invalid state <state>
Explanation	Internal Error, the fragmented IP packet has an invalid state.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	state
Context Parameters	Dropped Fragments Rule Name

2.13.12. drop_duplicate_frag_suspect_packet (ID: 02000012)

Default Severity	WARNING
Log Message	Dropping duplicate fragment of suspect packet
Explanation	A duplicate fragment of an IP packet, which may contain illegal fragments, was received. Dropping the duplicate fragment.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.13. drop_duplicate_frag (ID: 02000013)

Default Severity	WARNING
Log Message	Dropping duplicate fragment
Explanation	A duplicate fragment of an IP packet was received. Dropping the duplicate fragment.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.14. frag_offset_plus_length_not_in_range (ID: 02000014)

Default Severity	ERROR
Log Message	Fragment offset+length not in range <minipdatalen>-<maxipdatalen>
Explanation	The fragment offset and length would be outside of the allowed IP size range. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	minipdatalen maxipdatalen
Context Parameters	Rule Name Packet Buffer

2.13.15. no_available_fragacts (ID: 02000015)

Default Severity	WARNING
Log Message	Internal Error: No available resources (out of memory?).
Explanation	An Internal Error occurred. Failed to create necessary fragmentation reassembly resources. This could be a result of the unit being out of memory.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.16. bad_ipdatalen (ID: 02000016)

Default Severity	ERROR
Log Message	Bad IPDataLen=<ipdatalen>
Explanation	The partly reassembled IP packet has an invalid IP data length. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipdatalen
Context Parameters	Rule Name Packet Buffer

2.13.17. bad_ipdatalen (ID: 02000017)

Default Severity	ERROR
Log Message	Fragment offset+length is greater than the configured maximum <maxipdatalen>
Explanation	The fragment offset plus length would result in a greater length than the configured maximum length of an IP packet. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	maxipdatalen
Context Parameters	Rule Name Packet Buffer

2.13.18. overlapping_frag (ID: 02000018)

Default Severity	ERROR
Log Message	Overlapping fragment
Explanation	This fragment would overlap the next fragment offset. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.19. bad_offs (ID: 02000019)

Default Severity	ERROR
Log Message	Bad fragment offset
Explanation	The fragment has an invalid offset. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.20. duplicate_frag_with_different_length (ID: 02000020)

Default Severity	ERROR
Log Message	Duplicate fragment with different length received
Explanation	The fragment is a duplicate of an already received fragment, but the fragment lengths differ. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.21. duplicate_frag_with_different_data (ID: 02000021)

Default Severity	ERROR
Log Message	Duplicate fragment with different data received
Explanation	The fragment is a duplicate of an already received fragment, but the fragment data differs. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.22. partial_overlap (ID: 02000022)

Default Severity	ERROR
Log Message	Fragments partially overlap
Explanation	Two fragments partially overlap. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.23. drop_frag_disallowed_suspect_packet (ID: 02000023)

Default Severity	WARNING
Log Message	Dropping fragment of disallowed suspect packet
Explanation	A fragment of a disallowed IP packet, which may contain illegal fragments, is dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.24. drop_frag_disallowed_packet (ID: 02000024)

Default Severity	WARNING
Log Message	Dropping fragment of disallowed packet
Explanation	A fragment of a disallowed IP packet is dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.25. already_completed (ID: 02000025)

Default Severity	ERROR
-------------------------	-------

Log Message	Dropping extraneous fragment of completed packet
Explanation	A completed reassembled IP packet contains a extraneous fragment, which is dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.26. drop_frag_failed_suspect_packet (ID: 02000026)

Default Severity	WARNING
Log Message	Dropping fragment of failed suspect packet
Explanation	A fragment of a failed IP packet, which may contain illegal fragments, is dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.27. drop_frag_failed_packet (ID: 02000027)

Default Severity	WARNING
Log Message	Dropping fragment of failed packet
Explanation	A fragment of a failed IP packet is dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.28. drop_frag_illegal_packet (ID: 02000028)

Default Severity	WARNING
Log Message	Dropping fragment of illegal packet
Explanation	A fragment of an illegal IP packet is dropped.

Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.13.29. fragments_available_freeing (ID: 02000100)

Default Severity	CRITICAL
Log Message	Internal Error: Contains fragments even when freeing. Dropping
Explanation	An Internal Error occured when freeing an active fragment. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Dropped Fragments Rule Name

2.14. GRE

These log messages refer to the **GRE (GRE events)** category.

2.14.1. failed_to_setup_gre_tunnel (ID: 02200001)

Default Severity	WARNING
Log Message	Failed to setup open tunnel from <local_ip> to <remote_ip>
Explanation	Unable to setup GRE tunnel with endpoint.
Gateway Action	drop
Recommended Action	Check CONN usage and local routing.
Revision	1
Parameters	local_ip remote_ip

2.14.2. gre_bad_flags (ID: 02200002)

Default Severity	WARNING
Log Message	GRE packet with bad flag(s). Packet dropped
Explanation	Received GRE packet with a bad flag combination.
Gateway Action	drop
Recommended Action	Check GRE endpoint configuration.
Revision	1
Context Parameters	Packet Buffer

2.14.3. gre_bad_version (ID: 02200003)

Default Severity	WARNING
Log Message	GRE packet with bad version (not 0). Packet dropped
Explanation	Received GRE packet with bad version.
Gateway Action	drop
Recommended Action	Check GRE endpoint configuration.
Revision	1
Context Parameters	Packet Buffer

2.14.4. gre_checksum_error (ID: 02200004)

Default Severity	WARNING
Log Message	GRE packet with checksum error. Packet dropped
Explanation	Received GRE packet with checksum errors.
Gateway Action	drop
Recommended Action	Check network equipment for errors.
Revision	1
Context Parameters	Packet Buffer

2.14.5. gre_length_error (ID: 02200005)

Default Severity	WARNING
Log Message	GRE packet length error. Packet dropped
Explanation	Received GRE packet with length error.
Gateway Action	drop
Recommended Action	Check GRE endpoint configuration.
Revision	1
Context Parameters	Packet Buffer

2.14.6. gre_send_routing_loop_detected (ID: 02200006)

Default Severity	WARNING
Log Message	Routing loop detected. GRE packet send failed
Explanation	Routing loop to the GRE endpoint detected.
Gateway Action	drop
Recommended Action	Check local routing.
Revision	1
Context Parameters	Packet Buffer

2.14.7. unmatched_session_key (ID: 02200007)

Default Severity	WARNING
Log Message	Received GRE packet with unmatched session key. Packet dropped
Explanation	Received GRE packet with unmatched session key.
Gateway Action	drop
Recommended Action	Check GRE session key settings on the remote gateway.

Revision	1
Parameters	session_key
Context Parameters	Packet Buffer

2.14.8. gre_routing_flag_set (ID: 02200008)

Default Severity	WARNING
Log Message	Received GRE packet with routing flag set. Packet dropped
Explanation	Received GRE packet with unsupported routing option enabled.
Gateway Action	drop
Recommended Action	Check GRE configuration on remote gateway.
Revision	1
Context Parameters	Packet Buffer

2.15. HA

These log messages refer to the **HA (High Availability events)** category.

2.15.1. peer_gone (ID: 01200001)

Default Severity	NOTICE
Log Message	Peer firewall disappeared. Going active
Explanation	The peer gateway (which was active) is not available anymore. This gateway will now go active instead.
Gateway Action	activate
Recommended Action	None.
Revision	1

2.15.2. peer_gone (ID: 01200002)

Default Severity	NOTICE
Log Message	Peer firewall disappeared.
Explanation	The peer gateway (which was inactive) is not available anymore. This gateway will continue to stay active.
Gateway Action	None
Recommended Action	None.
Revision	1

2.15.3. conflict_both_peers_active (ID: 01200003)

Default Severity	NOTICE
Log Message	Conflict: Both peers are active! Resolving...
Explanation	A conflict occurred as both peers are active at the same time. The conflict will automatically be resolved.
Gateway Action	resolving
Recommended Action	None.
Revision	1

2.15.4. peer_has_higher_local_load (ID: 01200004)

Default Severity	NOTICE
Log Message	Both active, peer has higher local load; staying active

Explanation	Both members are active, but the peer has higher local load. This gateway will stay active.
Gateway Action	stay_active
Recommended Action	None.
Revision	1

2.15.5. peer_has_lower_local_load (ID: 01200005)

Default Severity	NOTICE
Log Message	Both active, peer has lower local load; deactivating
Explanation	Both members are active, but the peer has lower local load. This gateway will de-activate.
Gateway Action	deactivate
Recommended Action	None.
Revision	1

2.15.6. peer_has_more_connections (ID: 01200006)

Default Severity	NOTICE
Log Message	Both active, peer has more connections; deactivating
Explanation	Both members are active, but the peer has more connections. This gateway will de-activate.
Gateway Action	deactivate
Recommended Action	None.
Revision	1

2.15.7. peer_has_fewer_connections (ID: 01200007)

Default Severity	NOTICE
Log Message	Both active, peer has fewer connections; staying active
Explanation	Both members are active, but the peer has fewer connections. This gateway will stay active.
Gateway Action	stay_active
Recommended Action	None.
Revision	1

2.15.8. conflict_both_peers_inactive (ID: 01200008)

Default Severity	NOTICE
Log Message	Conflict: Both peers are inactive! Resolving...
Explanation	A conflict occurred as both peers are inactive at the same time. The conflict will automatically be resolved.
Gateway Action	None
Recommended Action	None.
Revision	1

2.15.9. peer_has_more_connections (ID: 01200009)

Default Severity	NOTICE
Log Message	Both inactive, peer has more connections; staying inactive...
Explanation	Both members are inactive, but the peer has more connections. This gateway will stay inactive.
Gateway Action	stay_deactivated
Recommended Action	None.
Revision	1

2.15.10. peer_has_fewer_connections (ID: 01200010)

Default Severity	NOTICE
Log Message	Both inactive, peer has fewer connections; going active...
Explanation	Both members are inactive, but the peer has fewer connections. This gateway will go active.
Gateway Action	activate
Recommended Action	None.
Revision	1

2.15.11. peer_alive (ID: 01200011)

Default Severity	NOTICE
Log Message	Peer firewall is alive
Explanation	The peer gateway is alive.
Gateway Action	None
Recommended Action	None.
Revision	1

2.15.12. heartbeat_from_unknown (ID: 01200043)

Default Severity	WARNING
Log Message	Received HA heartbeat from unknown IP. Dropping
Explanation	The received HA heartbeat packet was originating from an unknown IP. The packet will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.15.13. should_have_arrived_on_sync_iface (ID: 01200044)

Default Severity	WARNING
Log Message	This packet should have arrived on the sync iface. Dropping
Explanation	The HA packet did not arrive on the sync interface. The packet will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.15.14. activate_failed (ID: 01200050)

Default Severity	WARNING
Log Message	Failed to activate the configuration merged from HA partner
Explanation	The gateway failed to activate the merged configuration that was received from the peer.
Gateway Action	ha_activate_conf
Recommended Action	None.
Revision	1

2.15.15. merge_failed (ID: 01200051)

Default Severity	WARNING
Log Message	Failed to merge configuration from HA partner
Explanation	The gateway failed to merge the configuration that was received from the peer.
Gateway Action	ha_merge_conf
Recommended Action	None.
Revision	1

2.15.16. ha_commit_error (ID: 01200052)

Default Severity	WARNING
Log Message	The merged HA configuration contains errors
Explanation	The merged HA configuration contains errors, and can not be committed.
Gateway Action	ha_committchanges
Recommended Action	Resolve the errors and commit the changes again.
Revision	1

2.15.17. ha_write_failed (ID: 01200053)

Default Severity	WARNING
Log Message	Could not write HA configuration to disk
Explanation	The HA configuration could not be written to the storate media.
Gateway Action	ha_committchanges
Recommended Action	Verify that the storage media is not write protected or damaged.
Revision	1

2.15.18. ha_commit_unknown_error (ID: 01200054)

Default Severity	WARNING
Log Message	An unknown error occured while saving the HA configuration
Explanation	An unknown error occured when the HA configuration was to be saved. It has not been committed.
Gateway Action	ha_committchanges
Recommended Action	None.
Revision	1

2.15.19. resync_conns_to_peer (ID: 01200100)

Default Severity	WARNING
Log Message	Initiating complete resynchronization of <numconns> connections to peer firewall
Explanation	All current connections will be re-synchronized to peer, as the peer has been restarted. Initializing re-synchronization process.
Gateway Action	resync_conns_init
Recommended Action	None.
Revision	1
Parameters	reason numconns

2.15.20. hasync_connection_established (ID: 01200200)

Default Severity	NOTICE
Log Message	HASync connection to peer firewall established
Explanation	HA synchronization connection to peer has been established. Supported events will now be synchronized between the members of the HA cluster.
Gateway Action	None
Recommended Action	None.
Revision	1

2.15.21. hasync_connection_disconnected_lifetime_expired (ID: 01200201)

Default Severity	NOTICE
Log Message	HASync connection lifetime expired. Reconnecting...
Explanation	The HA synchronization connection lifetime has expired. A new connection will be established by reconnecting to the peer.
Gateway Action	reconnect
Recommended Action	None.
Revision	1

2.15.22. hasync_connection_failed_timeout (ID: 01200202)

Default Severity	NOTICE
-------------------------	--------

Log Message	HASync connection to peer firewall failed. Reconnecting...
Explanation	The HA synchronization connection attempt failed. Reconnecting to peer.
Gateway Action	reconnect
Recommended Action	None.
Revision	1

2.15.23. resync_conns_to_peer_complete (ID: 01200300)

Default Severity	NOTICE
Log Message	Connection resynchronization to peer complete
Explanation	The connection resynchronization process to peer is complete. All connections has been synchronized.
Gateway Action	None
Recommended Action	None.
Revision	1

2.15.24. disallowed_on_sync_iface (ID: 01200400)

Default Severity	WARNING
Log Message	Received non-HA traffic on sync iface. Dropping
Explanation	A packet which is not a HA-related packet was received on the sync interface. This should not happend, and the packet will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.15.25. sync_packet_on_nonsync_iface (ID: 01200410)

Default Severity	WARNING
Log Message	Received state sync packet on non-sync iface. Dropping
Explanation	A HA state sync packet was recieved on a non-sync interface. This should never happend, and the packet will be dropped.
Gateway Action	drop
Recommended Action	None.

Revision	1
Context Parameters	Rule Name Packet Buffer

2.15.26. ttl_too_low (ID: 01200411)

Default Severity	WARNING
Log Message	Received HA heartbeat with too low TTL. Dropping
Explanation	The received HA heartbeat packet had a TTL (Time-To-Live) field which is too low. The packet will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.15.27. heartbeat_from_myself (ID: 01200412)

Default Severity	WARNING
Log Message	Received HA heartbeat from the gateway itself. Dropping
Explanation	The received HA heartbeat packet was originating from the gateway itself. The packet will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.15.28. config_sync_failure (ID: 01200500)

Default Severity	CRITICAL
Log Message	Tried to synchronize configuration to peer 3 times without success. Giving up.
Explanation	The gateway tried to synchronize the configuration to peer three times, but failed. It will now give up trying to do so.
Gateway Action	give_up_synching
Recommended Action	None.
Revision	1

Parameters	numretries
------------	------------

2.15.29. action=deactivate reason=requested (ID: 01200616)

Default Severity	NOTICE
Log Message	Both active, deactivation in progress.
Explanation	Both active, deactivation in progress.
Gateway Action	None
Recommended Action	None.
Revision	1

2.15.30. action=activate reason=requested (ID: 01200617)

Default Severity	NOTICE
Log Message	Both not active, activation in progress.
Explanation	Both not active, activation in progress.
Gateway Action	None
Recommended Action	None.
Revision	1

2.15.31. action=going_online (ID: 01200618)

Default Severity	NOTICE
Log Message	Ha unit going online.
Explanation	Ha unit going online.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	previous_shutdown=

2.16. HWM

These log messages refer to the **HWM (Hardware monitor events)** category.

2.16.1. temperature_alarm (ID: 04000011)

Default Severity	WARNING
Log Message	Temperature monitor <index> (<name>) is outside the specified limit. Current value is <current_temp> <unit>, lower limit is <min_limit>, upper limit is <max_limit>
Explanation	The unit may be overheating, this may be because the cooling is failing or to hot enviroment.
Gateway Action	none
Recommended Action	Shutdown the unit and determine the problem.
Revision	1
Parameters	index name unit current_temp min_limit max_limit

2.16.2. temperature_normal (ID: 04000012)

Default Severity	WARNING
Log Message	Temperature monitor <index> (<name>) is outside the specified limit. Current value is <current_temp> <unit>, lower limit is <min_limit>, upper limit is <max_limit>
Explanation	The sensor reports that the temperature value is back in the normal range.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	index name unit current_temp min_limit max_limit

2.16.3. voltage_alarm (ID: 04000021)

Default Severity	WARNING
-------------------------	---------

Log Message	Voltage monitor <index> (<name>) is outside the specified limit. Current value is <current_voltage> <unit>, lower limit is <min_limit>, upper limit is <max_limit>
Explanation	The powersupply of this unit may be failing.
Gateway Action	none
Recommended Action	Change powersupply unit.
Revision	1
Parameters	index name unit current_voltage min_limit max_limit

2.16.4. voltage_normal (ID: 04000022)

Default Severity	WARNING
Log Message	Voltage monitor <index> (<name>) is outside the specified limit. Current value is <current_voltage> <unit>, lower limit is <min_limit>, upper limit is <max_limit>
Explanation	The sensor reports that the voltage value is back in the normal range.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	index name unit current_voltage min_limit max_limit

2.16.5. fanrpm_alarm (ID: 04000031)

Default Severity	WARNING
Log Message	Fan RPM monitor <index> (<name>) is outside the specified limit. Current value is <current_fanrpm> <unit>, value is <current_fanrpm> <unit>, lower limit is <min_limit>, upper limit is <max_limit>
Explanation	The fan is behaving strange, this may because it is failing or blocked.
Gateway Action	none
Recommended Action	Unblock or change the corresponding fan.
Revision	1
Parameters	index

name
unit
current_fanrpm
min_limit
max_limit

2.16.6. fanrpm_normal (ID: 04000032)

Default Severity	WARNING
Log Message	Fan RPM monitor <index> (<name>) is outside the specified limit. Current value is <current_fanrpm> <unit>, lower limit is <min_limit>, upper limit is <max_limit>
Explanation	The sensor reports that the fan rpm value is back in the normal range.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	index name unit current_fanrpm min_limit max_limit

2.16.7. gpio_alarm (ID: 04000041)

Default Severity	WARNING
Log Message	GPIO monitor <index> (<name>) is outside the specified limit. Current value is <current_gpio> <unit>, value is <current_gpio> <unit>, lower limit is <min_limit>, upper limit is <max_limit>
Explanation	This varies depending on hardware model and what the GPIO is connected to.
Gateway Action	none
Recommended Action	Depends on what the GPIO is connected to.
Revision	1
Parameters	index name unit current_gpio min_limit max_limit

2.16.8. gpio_normal (ID: 04000042)

Default Severity	WARNING
-------------------------	---------

Log Message	Temperature monitor <index> (<name>) is outside the specified limit. Current value is <current_gpio> <unit>, lower limit is <min_limit>, upper limit is <max_limit>
Explanation	The sensor reports that the GPIO value is back into the normal range.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	index name unit current_gpio min_limit max_limit

2.16.9. free_memory_warning_level (ID: 04000101)

Default Severity	WARNING
Log Message	Free memory has fallen below the specified limit of <limit_percentage> percent, limit classified is <severity>, free <free_mem> MB of total <total_mem> MB, percentage free <free_percentage>
Explanation	The amount of free memory is getting low.
Gateway Action	None
Recommended Action	Review the configuration and disable or lower settings to reduce memory consumption.
Revision	1
Parameters	limit_percentage total_mem free_mem free_percentage severity

2.16.10. free_memory_warning_level (ID: 04000102)

Default Severity	WARNING
Log Message	Free memory has fallen below the specified limit of <limit_megabyte> megabyte, limit classified is <severity>, free <free_mem> MB of total <total_mem> MB, percentage free <free_percentage>
Explanation	The amount of free memory is getting low.
Gateway Action	None
Recommended Action	Review the configuration and disable or lower settings to reduce memory consumption.
Revision	1

Parameters	limit_megabyte total_mem free_mem free_percentage severity
-------------------	--

2.16.11. free_memory_normal_level (ID: 04000103)

Default Severity	NOTICE
Log Message	The amount of free memory is in the normal range, free <free_mem> MB of total <total_mem> MB, percentage free <free_percentage>
Explanation	The memory usage is in the normal range.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	total_mem free_mem free_percentage

2.17. IDP

These log messages refer to the **IDP (Intrusion Detection & Prevention events)** category.

2.17.1. scan_detected (ID: 01300001)

Default Severity	NOTICE
Log Message	Scan detected: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Closing connection.
Explanation	A scan signature mapped to the "protect" action matched the traffic, closing connection.
Gateway Action	close
Recommended Action	Research the advisory (searchable by the unique ID), if you suspect an attack.
Revision	1
Parameters	description signatureid idrule ipproto srcip srcport destip destport
Context Parameters	Rule Name Deep Inspection

2.17.2. idp_notice (ID: 01300002)

Default Severity	WARNING
Log Message	IDP Notice: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Closing connection.
Explanation	A notice signature mapped to the "protect" action matched the traffic, closing connection.
Gateway Action	close
Recommended Action	This is probably not an attack, but you may research the advisory (searchable by the unique ID).
Revision	1
Parameters	description signatureid idrule ipproto srcip

	srcport destip destport
Context Parameters	Rule Name Deep Inspection

2.17.3. intrusion_detected (ID: 01300003)

Default Severity	WARNING
Log Message	Intrusion detected: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Closing connection.
Explanation	An attack signature mapped to the "protect" action matched the traffic.
Gateway Action	close
Recommended Action	Research the advisory (searchable by the unique ID).
Revision	1
Parameters	description signatureid idrule ipproto srcip srcport destip destport
Context Parameters	Rule Name Deep Inspection

2.17.4. virus_detected (ID: 01300004)

Default Severity	WARNING
Log Message	Virus/worm detected: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Closing connection.
Explanation	A virus signature mapped to the "protect" action matched the traffic.
Gateway Action	close
Recommended Action	Research the advisory (searchable by the unique ID).
Revision	1
Parameters	description signatureid idrule ipproto srcip srcport

	destip destport
Context Parameters	Rule Name Deep Inspection

2.17.5. scan_detected (ID: 01300005)

Default Severity	NOTICE
Log Message	Scan detected: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>.
Explanation	A scan signature matched the traffic.
Gateway Action	None
Recommended Action	Research the advisory (searchable by the unique ID).
Revision	1
Parameters	description signatureid idrule ipproto srcip srcport destip destport
Context Parameters	Rule Name Deep Inspection

2.17.6. idp_notice (ID: 01300006)

Default Severity	NOTICE
Log Message	IDP Notice: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>.
Explanation	A notice signature matched the traffic.
Gateway Action	None
Recommended Action	This is probably not an attack, but you may research the advisory (searchable by the unique ID).
Revision	1
Parameters	description signatureid idrule ipproto srcip srcport destip destport

Context Parameters	Rule Name Deep Inspection
---------------------------	------------------------------

2.17.7. intrusion_detected (ID: 01300007)

Default Severity	NOTICE
Log Message	Intrusion detected: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>.
Explanation	An attack signature matched the traffic.
Gateway Action	None
Recommended Action	Research the advisory (searchable by the unique ID).
Revision	1
Parameters	description signatureid idrule ipproto srcip srcport destip destport
Context Parameters	Rule Name Deep Inspection

2.17.8. virus_detected (ID: 01300008)

Default Severity	NOTICE
Log Message	Virus/Worm detected: <description>, Signature ID=<signatureid>. ID Rule: <idrule>. Protocol: <ipproto>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>.
Explanation	A virus signature matched the traffic.
Gateway Action	None
Recommended Action	Research the advisory (searchable by the unique ID).
Revision	1
Parameters	description signatureid idrule ipproto srcip srcport destip destport
Context Parameters	Rule Name Deep Inspection

2.17.9. invalid_url_format (ID: 01300009)

Default Severity	ERROR
Log Message	Failed to parse the HTTP URL. ID Rule: <idrule>. URL: <url>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Closing connection.
Explanation	The unit failed parsing an URL. The reason for this is probably because the URL has an invalid format, or it contains invalid UTF8 formatted characters.
Gateway Action	close
Recommended Action	Make sure that the URL is formatted correctly.
Revision	1
Parameters	idrule url srcip srcport destip destport
Context Parameters	Rule Name

2.17.10. invalid_url_format (ID: 01300010)

Default Severity	WARNING
Log Message	Failed to parse the HTTP URL. ID Rule: <idrule>. URL: <url>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Ignoring the URL.
Explanation	The unit failed parsing an URL. The reason for this is probably because the URL has an invalid format, or it contains invalid UTF8 formatted characters.
Gateway Action	ignore
Recommended Action	Make sure that the URL is formatted correctly.
Revision	1
Parameters	idrule url srcip srcport destip destport
Context Parameters	Rule Name

2.17.11. idp_evasion (ID: 01300011)

Default Severity	ERROR
-------------------------	-------

Log Message	Failed to reassemble data. ID Rule: <idrule>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Closing connection.
Explanation	The unit failed to reassemble data. The reason for this is probably due to an IDP engine evasion attack.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	idrule srcip srcport destip destport
Context Parameters	Rule Name

2.17.12. idp_evasion (ID: 01300012)

Default Severity	ERROR
Log Message	Failed to reassemble data. ID Rule: <idrule>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>.
Explanation	The unit failed to reassemble data. The reason for this is probably due to an IDP engine evasion attack.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	idrule srcip srcport destip destport
Context Parameters	Rule Name

2.17.13. idp_outofmem (ID: 01300013)

Default Severity	ERROR
Log Message	Failed to scan data. ID Rule: <idrule>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Closing connection.
Explanation	The unit failed to scan data. The reason for this is due to low amount of memory.
Gateway Action	close

Recommended Action	Review your configuration.
Revision	1
Parameters	idrule srcip srcport destip destport
Context Parameters	Rule Name

2.17.14. idp_outofmem (ID: 01300014)

Default Severity	ERROR
Log Message	Failed to scan data. ID Rule: <idrule>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>.
Explanation	The unit failed to scan data. The reason for this is due to low amount of memory.
Gateway Action	ignore
Recommended Action	Review your configuration.
Revision	1
Parameters	idrule srcip srcport destip destport
Context Parameters	Rule Name

2.17.15. idp_failscan (ID: 01300015)

Default Severity	ERROR
Log Message	Failed to scan data. ID Rule: <idrule>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Reason: reason>. Closing connection.
Explanation	The unit failed to scan data.
Gateway Action	close
Recommended Action	None.
Revision	1
Parameters	idrule srcip srcport destip destport reason

Context Parameters Rule Name

2.17.16. idp_failscan (ID: 01300016)

Default Severity ERROR

Log Message Failed to scan data. ID Rule: <idrule>. Source IP: <srcip>. Source Port: <srcport>. Destination IP: <destip>. Destination Port: <destport>. Reason: <reason>.

Explanation The unit failed to scan data.

Gateway Action ignore

Recommended Action None.

Revision 1

Parameters idrule
srcip
srcport
destip
destport
reason

Context Parameters Rule Name

2.18. IDPUPDATE

These log messages refer to the **IDPUPDATE (Intrusion Detection & Prevention Database update)** category.

2.18.1. idp_db_update_failure (ID: 01400001)

Default Severity	ALERT
Log Message	Update of the Intrusion Detection & Prevention database failed, because of <reason>
Explanation	The unit tried to update the Intrusion Detection & Prevention database, but failed. The reason for this is specified in the "reason" parameter.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.18.2. idp_database_downloaded (ID: 01400002)

Default Severity	NOTICE
Log Message	New Intrusion Detection & Prevention database downloaded
Explanation	An updated version of the Intrusion Detection & Prevention database has been downloaded, which will now be used.
Gateway Action	using_new_database
Recommended Action	None.
Revision	2

2.18.3. idp_db_already_up_to_date (ID: 01400003)

Default Severity	NOTICE
Log Message	Intrusion Detection & Prevention database is up-to-date
Explanation	The current Intrusion Detection & Prevention database is up-to-date, and does not need to be updated.
Gateway Action	None
Recommended Action	None.
Revision	1

2.18.4. idp_db_update_denied (ID: 01400004)

Default Severity	NOTICE
Log Message	Intrusion Detection & Prevention database could not be updated, as no valid subscription exist
Explanation	The current license does not allow Intrusion Detection & Prevention database to be updated.
Gateway Action	None
Recommended Action	Check the system's time and/or purchase a subscription.
Revision	1

2.18.5. idp_detects_invalid_system_time (ID: 01400005)

Default Severity	ERROR
Log Message	System clock is not properly set. Invalid date (<date>) in IDP signature file. IDP disabled
Explanation	The system clock is not up to date. The system clock must be set correctly in order to use the IDP features. IDP features remains disabled until clock is correct and a manual IDP update has been performed.
Gateway Action	idp_disabled
Recommended Action	Check and set the system time correct and perform a manual IDP update.
Revision	1
Parameters	date

2.18.6. downloading_new_database (ID: 01400007)

Default Severity	NOTICE
Log Message	Downloading new IDP database
Explanation	A new IDP database is available. The database is being downloaded.
Gateway Action	downloading_new_database
Recommended Action	None.
Revision	1

2.18.7. unsynced_databases (ID: 01400009)

Default Severity	WARNING
Log Message	Unsynchronized hardware and software databases detected
Explanation	The IDP hardware and software databases are not synchronized. A full

	update is automatically initiated.
Gateway Action	downloading_new_database
Recommended Action	None.
Revision	1

2.19. IFACEMON

These log messages refer to the **IFACEMON (Interface monitor events)** category.

2.19.1. ifacemon_status_bad_rereport (ID: 03900001)

Default Severity	NOTICE
Log Message	IfaceMon reset interface <iface> 10 seconds ago. Link status: <linkspeed> Mbps <duplex> duplex
Explanation	The Interface Monitor reset the interface 10 seconds ago.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	delay iface [linkspeed] [duplex]

2.19.2. ifacemon_status_bad (ID: 03900003)

Default Severity	WARNING
Log Message	IfaceMon reports interface problems on <iface>. Resetting interface. Link status: <linkspeed> Mbps <duplex> duplex
Explanation	The Interface Monitor has discovered problems on an interface, and will reset it.
Gateway Action	nic_reset
Recommended Action	None.
Revision	1
Parameters	iface linkspeed duplex

2.19.3. ifacemon_status_bad (ID: 03900004)

Default Severity	WARNING
Log Message	IfaceMon reports interface problems on <iface> Resetting interface
Explanation	The Interface Monitor has discovered problems on an interface, and will reset it.
Gateway Action	nic_reset
Recommended Action	None.

Revision	1
Parameters	iface [linkspeed] [duplex]

2.20. IGMP

These log messages refer to the **IGMP (IGMP events)** category.

2.20.1. querier_election_won (ID: 04200001)

Default Severity	NOTICE
Log Message	Taking on the role of Querier at interface <iface>.
Explanation	This router is now the IGMP Querier at the specified interface.
Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	iface

2.20.2. querier_election_lost (ID: 04200002)

Default Severity	NOTICE
Log Message	Lost Querier election to <dest> at interface <iface>.
Explanation	"I" am no longer the IMGP Querier at the specified interface.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	dest iface

2.20.3. invalid_dest_ip_address (ID: 04200003)

Default Severity	WARNING
Log Message	Rejected IGMP message directed to unicast IP <ip_dest> at interface <recv_if>.
Explanation	Rejected IGMP message directed to a unicast IP. Possible IGMP DoS attack. Note that sending IGMP messages to a unicast IP is legal with IGMPv1 and IGMPv2, but not recommended.
Gateway Action	drop
Recommended Action	Identify the offending application, upgrade if possible.
Revision	1
Parameters	recv_if ip_dest

Context Parameters Packet Buffer

2.20.4. invalid_destination_ethernet_address (ID: 04200004)

Default Severity	WARNING
Log Message	Rejected IGMP message with inconsistent IP/ethernet addresses (<ipdest>/<edest>) at interface <recv_if>.
Explanation	Rejected IGMP message directed to a unicast ethernet. Known IGMP DoS attack.
Gateway Action	drop
Recommended Action	Identify the offending application or user, isolate or upgrade if possible.
Revision	1
Parameters	recv_if ipdest edest
Context Parameters	Packet Buffer

2.20.5. failed_restarting_igmp_conn (ID: 04200006)

Default Severity	EMERG
Log Message	Could not restart the IGMP listening conn. Reason: Out of memory
Explanation	Could not restart the IGMP listening conn. The IGMP system is no longer functional since it cannot handle IGMP requests.
Gateway Action	None
Recommended Action	Reboot the system.
Revision	1

2.20.6. invalid_size_query_packet (ID: 04200007)

Default Severity	WARNING
Log Message	Broken IGMP Query at interface <recv_if> (payload exceeds packet size).
Explanation	Harmful condition that potentially could give an attacker full access to the system. May indicate faulty hardware, an attack or experimental software.
Gateway Action	drop
Recommended Action	None, but keep an eye open for malfunctional software/hardware somewhere on the network.

Revision	1
Parameters	recv_if
Context Parameters	Packet Buffer

2.20.7. invalid_query_group_address (ID: 04200008)

Default Severity	ERROR
Log Message	IGMP group specific query at interface <recv_if> about group <grp> (<grp_sat> after being SAT'ed) includes unicast ip address.
Explanation	Unicast IP address found inside group specific query. This is most likely a faulty SAT config.
Gateway Action	drop
Recommended Action	Check your IGMP ruleset to see if a muticast group somehow might be translated into a unicast address.
Revision	1
Parameters	recv_if grp grp_sat
Context Parameters	Packet Buffer

2.20.8. igmp_query_dropped (ID: 04200009)

Default Severity	NOTICE
Log Message	Rule <name> dropped IGMP Query about group <grp> and source <src> at interface <if> from router <rip>.
Explanation	Dropped IGMP Query.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	if rip igmpver grp src name

2.20.9. igmp_query_received (ID: 04200010)

Default Severity	NOTICE
Log Message	Rule <name> <action> IGMP Query about group <grp> and source <src> at interface <if> from router <rip>. Group <grp> is translated

	into <sgrp> and source <src> into <ssrc>.
Explanation	Got IGMP Query.
Gateway Action	allow
Recommended Action	None.
Revision	1
Parameters	if rip igmpver grp src sgrp ssrc name action

2.20.10. bad_src (ID: 04200011)

Default Severity	WARNING
Log Message	Rule <name> drops multicast sender <src> (SAT'ed into <sats>) in group <grp> (SAT'ed into <satg>) specific IGMP Query at interface <iface>.
Explanation	This is most likely a faulty IGMP configuration, but may also indicate faulty software on the network. Under special circumstances this could be an active attempt to scan the network for information.
Gateway Action	drop
Recommended Action	Specifically check your IGMP ruleset for incorrect SAT information (IGMP support requires at least one "REPORT" (Member Report) rule and one matching "QUERY" rule). Make sure both multicast groups and source addresses map one-to-one between Member Reports and Queries. Finally check the network for for other anomalies that could indicate broken equipment or installed "spyware".
Revision	1
Parameters	name src grp sats satg iface

2.20.11. igmp_report_received (ID: 04200012)

Default Severity	NOTICE
Log Message	Rule <name> <action> IGMP Member Report concerning group <grp> and source <src> at interface <if> from host <hip>. Group <grp> is translated into <sgrp> and source <src> into <ssrc>
Explanation	Got IGMP Report.

Gateway Action	allow
Recommended Action	None.
Revision	1
Parameters	if hip igmpver grp src sgrp ssrc name action

2.20.12. packet_includes_aux_data (ID: 04200013)

Default Severity	WARNING
Log Message	IGMP Group record <grp> from interface <recv_if> contains auxilliary data.
Explanation	This software support IGMPv1, IGMPv2 and IGMPv3 and none of them support the feature known as "Auxilliary Data". This is a broken packet.
Gateway Action	drop
Recommended Action	If this is a legal situation and the administrator have no reason to suspect an attack, upgrading this software may solve the problem.
Revision	1
Parameters	recv_if grp
Context Parameters	Packet Buffer

2.20.13. invalid_size_report_packet (ID: 04200014)

Default Severity	ERROR
Log Message	Broken IGMP Member Report at interface <recv_if>. Group record <grp> makes payload larger than IGMP packet size.
Explanation	Harmful condition that potentially could give an attacker full access to the system. May indicate faulty hardware, an attack or experimental software.
Gateway Action	drop
Recommended Action	None, but keep an eye open for for broken hardware somewhere in the network.
Revision	1
Parameters	recv_if grp

Context Parameters	Packet Buffer
--------------------	---------------

2.20.14. bad_grp (ID: 04200015)

Default Severity	WARNING
Log Message	Bad IGMP Member Report at interface <iface>: Group record request group <grp> (which is not a multicast group).
Explanation	This is most likely a faulty IGMP config.
Gateway Action	drop
Recommended Action	Specifically check for inconsistent SAT/NAT information in the IGMP config.
Revision	1
Parameters	grp iface

2.20.15. invalid_report_grp_record (ID: 04200016)

Default Severity	WARNING
Log Message	Bad IGMP Member Report received. Group record <grp> of unknown type <type>.
Explanation	This indicates faulty software/hardware somewhere on the network.
Gateway Action	drop
Recommended Action	None, but keep an eye open for for broken hardware somewhere in the network.
Revision	1
Parameters	grp type
Context Parameters	Packet Buffer

2.20.16. igmp_report_dropped (ID: 04200017)

Default Severity	NOTICE
Log Message	Rule <name> drops IGMP Member Report concerning group <grp> and source <src> at interface <if> from host <hip>.
Explanation	Dropped IGMP Report.
Gateway Action	drop
Recommended Action	None.
Revision	1

Parameters	if hip igmpver grp src sat_grp sat_src name
-------------------	--

2.20.17. igmp_ruleset_rejects_report (ID: 04200018)

Default Severity	WARNING
Log Message	Rule <name> drops multicast sender <src> for group record <grp> in Member Report at interface <iface>.
Explanation	IGMP Member Report contains an unwanted IP sender.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	name src grp iface

2.20.18. bad_inet (ID: 04200019)

Default Severity	WARNING
Log Message	Rejected IGMP message from incorrect IP <src> at interface <iface>.
Explanation	Rejected IGMP message because it claims to have been sent by "me", but I know I did not send any. Possible IGMP DoS attack, but more likely an IP conflict. .
Gateway Action	drop
Recommended Action	Assign a different IP to the offending application.
Revision	1
Parameters	src iface
Context Parameters	Packet Buffer

2.20.19. max_global_requests_per_second_reached (ID: 04200020)

Default Severity	WARNING
Log Message	Rejected IGMP message. Global requests per second rate reached

Explanation	Too many IGMP requests received per second. Possible IGMP DoS attack.
Gateway Action	drop
Recommended Action	Increase global IGMPMaxReqs per second limit if more requests are wanted.
Revision	1
Parameters	ipsrc iface

2.20.20. max_if_requests_per_second_reached (ID: 04200021)

Default Severity	WARNING
Log Message	Rejected IGMP message. Max requests per second and interface rate reached
Explanation	Too many IGMP requests received per second. Possible IGMP DoS attack.
Gateway Action	drop
Recommended Action	Increase IGMPMaxReqsIf per second limit if more requests are wanted.
Revision	1
Parameters	ipsrc iface

2.20.21. disallowed_igmp_version (ID: 04200022)

Default Severity	NOTICE
Log Message	Disallowed IGMP Version
Explanation	A system is using a too old IGMP version.
Gateway Action	drop
Recommended Action	Upgrade the host/router running the disallowed version, or lower LowestIGMPVer limit.
Revision	1
Parameters	recv_ver required_ver
Context Parameters	Packet Buffer

2.20.22. received_unknown_igmp_type (ID: 04200023)

Default Severity	NOTICE
-------------------------	--------

Log Message	Dropped IGMP message with unknown type.
Explanation	Invalid IGMP message type received.
Gateway Action	drop
Recommended Action	None, but keep an eye open for malfunctional software/hardware on the network.
Revision	1
Parameters	MSGType
Context Parameters	Packet Buffer

2.20.23. older_querier_present (ID: 04200024)

Default Severity	NOTICE
Log Message	Entering IGMPv<igmpver> Older Querier Present compatibility mode on interface <iface> because of a received General Query from <rip>.
Explanation	The router will use IGMPv[igmpver] when it is snooping/proxying IGMP messages upstream.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface rip igmpver

2.20.24. older_querier_gone (ID: 04200025)

Default Severity	NOTICE
Log Message	No IGMPv<igmpver> querier present. Older Querier Present (IGMPv<igmpver>) compatibility mode on interface <iface> has ended. Entering IGMPv<nigmpver> mode.
Explanation	The router has not heard any IGMPv[igmpver] general queries and will switch and use IGMPv[nigmpver] version when snooping/proxying IGMP messages upstream.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface igmpver nigmpver

2.21. IPPOOL

These log messages refer to the **IPPOOL (IPPool events)** category.

2.21.1. no_offer_received (ID: 01900001)

Default Severity	ERROR
Log Message	No offers were received
Explanation	No DHCP offers were received by the IP pool general query.
Gateway Action	None
Recommended Action	Review DHCP server parameters and IP pool configuration.
Revision	1
Parameters	waited
Context Parameters	Rule Name

2.21.2. no_valid_dhcp_offer_received (ID: 01900002)

Default Severity	ERROR
Log Message	No valid DHCP offers were received
Explanation	No valid DHCP offers were received.
Gateway Action	no_new_client_created
Recommended Action	Review DHCP server parameters and IP pool filters.
Revision	1
Context Parameters	Rule Name

2.21.3. too_many_dhcp_offers_received (ID: 01900003)

Default Severity	WARNING
Log Message	Too many DHCP offers received. This and subsequent offers will be ignored
Explanation	Too many DHCP offers received.
Gateway Action	ignoring_offer
Recommended Action	Limit the number of DHCP servers on the locally attached network.
Revision	1
Context Parameters	Rule Name

2.21.4. lease_disallowed_by_lease_filter (ID: 01900004)

Default Severity	WARNING
Log Message	The lease was rejected due to a lease filter
Explanation	A lease was rejected by a lease filter.
Gateway Action	lease_rejected
Recommended Action	Verify the lease filters.
Revision	1
Parameters	client_ip
Context Parameters	Rule Name

2.21.5. lease_disallowed_by_server_filter (ID: 01900005)

Default Severity	WARNING
Log Message	The lease was rejected due to a server filter
Explanation	A lease was rejected by a server filter.
Gateway Action	lease_rejected
Recommended Action	Verify the server filters.
Revision	1
Parameters	server_ip
Context Parameters	Rule Name

2.21.6. lease_have_bad_dhcp_server (ID: 01900006)

Default Severity	WARNING
Log Message	The lease was rejected due to a bad DHCP-server address
Explanation	A lease was rejected due to a bad DHCP server address.
Gateway Action	lease_rejected
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	client_ip
Context Parameters	Rule Name

2.21.7. lease_have_bad_netmask (ID: 01900007)

Default Severity	WARNING
-------------------------	---------

Log Message	The lease was rejected due to a bad offered netmask address
Explanation	A lease was rejected due to a bad offered netmask address.
Gateway Action	lease_rejected
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	netmask
Context Parameters	Rule Name

2.21.8. lease_have_bad_offered_broadcast (ID: 01900008)

Default Severity	WARNING
Log Message	The lease was rejected due to a bad offered broadcast address
Explanation	A lease was rejected due to a bad offered broadcast address.
Gateway Action	lease_rejected
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	broadcast
Context Parameters	Rule Name

2.21.9. lease_have_bad_offered_ip (ID: 01900009)

Default Severity	WARNING
Log Message	The lease was rejected due to a bad offered IP address
Explanation	A lease was rejected due to a bad offered IP address.
Gateway Action	lease_rejected
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	client_ip
Context Parameters	Rule Name

2.21.10. lease_have_bad_gateway_ip (ID: 01900010)

Default Severity	WARNING
Log Message	The lease was rejected due to a bad offered gateway address
Explanation	A lease was rejected due to a bad offered gateway address.

Gateway Action	lease_rejected
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	gateway_ip
Context Parameters	Rule Name

2.21.11. lease_ip_is_already_occupied (ID: 01900011)

Default Severity	WARNING
Log Message	The lease was rejected since it seem to be occupied
Explanation	A lease was rejected since it seem to be occupied.
Gateway Action	lease_rejected
Recommended Action	Check DHCP server configuration and statically configured hosts.
Revision	1
Parameters	client_ip
Context Parameters	Rule Name

2.21.12. lease_rejected_by_server (ID: 01900012)

Default Severity	WARNING
Log Message	The lease was rejected by server
Explanation	A lease was rejected by the DHCP server.
Gateway Action	lease_rejected
Recommended Action	Check DHCP server configuration.
Revision	1
Parameters	client_ip
Context Parameters	Rule Name

2.21.13. ip_offer_already_exist_in_the_pool (ID: 01900013)

Default Severity	WARNING
Log Message	The lease was rejected since the offered IP already exist in the pool
Explanation	A lease was rejected since the offered IP already exists in the pool.
Gateway Action	lease_rejected
Recommended Action	Check IP pool configuration.

Revision	1
Parameters	client_ip
Context Parameters	Rule Name

2.21.14. pool_reached_max_dhcp_clients (ID: 01900014)

Default Severity	ERROR
Log Message	The maximum number of clients for this IP pool have been reached
Explanation	The maximum number of clients for this pool have been reached.
Gateway Action	no_new_client_created
Recommended Action	Verify max clients limitation for the pool.
Revision	1
Context Parameters	Rule Name

2.21.15. macrange_depleted (ID: 01900015)

Default Severity	ERROR
Log Message	The range of MAC addresses for the DHCP clients have been depleted
Explanation	The configured range of MAC addresses for the DHCP clients have been depleted.
Gateway Action	no_new_client_created
Recommended Action	Expand the MAC address range.
Revision	1
Context Parameters	Rule Name

2.21.16. ip_fetched_pool (ID: 01900016)

Default Severity	NOTICE
Log Message	Subsystem fetched a IP from the pool
Explanation	A subsystem fetched an IP from the pool.
Gateway Action	inform
Recommended Action	None.
Revision	1
Parameters	client_ip subsystem
Context Parameters	Rule Name

2.21.17. ip_returned_to_pool (ID: 01900017)

Default Severity	NOTICE
Log Message	Subsystem returned an IP to the pool
Explanation	A subsystem returned an IP to the pool.
Gateway Action	inform
Recommended Action	None.
Revision	1
Parameters	client_ip subsystem
Context Parameters	Rule Name

2.22. IPSEC

These log messages refer to the **IPSEC (IPsec (VPN) events)** category.

2.22.1. fatal_ipsec_event (ID: 01800100)

Default Severity	ALERT
Log Message	Fatal event occurred, because of <reason>
Explanation	Fatal event occurred in IPsec stack.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.22.2. warning_ipsec_event (ID: 01800101)

Default Severity	WARNING
Log Message	Warning event occurred, because of <reason>
Explanation	Warning event from IPsec stack.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.22.3. audit_event (ID: 01800103)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	An audit event occurred in the IPsec stack.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.22.4. audit_flood (ID: 01800104)

Default Severity	NOTICE
Log Message	<reason>.
Explanation	The rate limit for audit messages was reached.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.22.5. ike_delete_notification (ID: 01800105)

Default Severity	NOTICE
Log Message	Local IP: <local_ip>, Remote IP: <remote_ip>, Cookies: <cookies>, Reason: <reason>.
Explanation	None.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	local_ip remote_ip cookies reason

2.22.6. ike_invalid_payload (ID: 01800106)

Default Severity	WARNING
Log Message	Local IP: <local_ip>, Remote IP: <remote_ip>, Cookies: <cookies>, Reason: <reason>.
Explanation	None.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	local_ip remote_ip cookies reason

2.22.7. ike_invalid_proposal (ID: 01800107)

Default Severity	WARNING
Log Message	Local IP: <local_ip>, Remote IP: <remote_ip>, Cookies: <cookies>, Reason: <reason>.
Explanation	The proposal for the security association could not be accepted.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	local_ip remote_ip cookies reason

2.22.8. ike_retry_limit_reached (ID: 01800108)

Default Severity	NOTICE
Log Message	Local IP: <local_ip>, Remote IP: <remote_ip>, Cookies: <cookies>, Reason: <reason>.
Explanation	The retry limit for transmitting ISAKMP messages was reached.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	local_ip remote_ip cookies reason

2.22.9. ike_quickmode_failed (ID: 01800109)

Default Severity	WARNING
Log Message	Local IP: <local_ip>, Remote IP: <remote_ip>, Cookies: <cookies>, Reason: <reason>.
Explanation	None.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	local_ip remote_ip cookies

reason

2.22.10. packet_corrupt (ID: 01800110)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	Received a corrupt packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.22.11. icv_failure (ID: 01800111)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	The computed and ICV of the received packet did not match.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.22.12. sequence_number_failure (ID: 01800112)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	The received packet did not fall within the sliding window.
Gateway Action	drop

Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.22.13. sa_lookup_failure (ID: 01800113)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	The received packet could not be mapped to an appropriate SA.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.22.14. ip_fragment (ID: 01800114)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	The packet offered to AH/ESP processing appears to be an IP fragment.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.22.15. sequence_number_overflow (ID: 01800115)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	An attempt to transmit a packet that would result in sequence number overflow.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.22.16. bad_padding (ID: 01800116)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	The received packet has incorrect padding.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.22.17. hardware_accelerator_congested (ID: 01800117)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	Hardware acceleration failed due to resource shortage.
Gateway Action	drop
Recommended Action	None.
Revision	1

Parameters	source_ip dest_ip spi seq protocol reason
-------------------	--

2.22.18. hardware_acceleration_failure (ID: 01800118)

Default Severity	NOTICE
Log Message	Source IP: <source_ip>, Destination IP: <dest_ip>, SPI: <spi>, Seq: <seq>, Protocol: <protocol>, Reason: <reason>.
Explanation	Hardware acceleration failed due to resource shortage, a corrupt packet or other hardware related error.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	source_ip dest_ip spi seq protocol reason

2.22.19. commit_failed (ID: 01800200)

Default Severity	CRITICAL
Log Message	Failed to commit IPsec configuration
Explanation	Failed to commit IPsec configuration.
Gateway Action	IPsec_configuration_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.22.20. commit_succeeded (ID: 01800201)

Default Severity	INFORMATIONAL
Log Message	Commit succeeded - recalculating flows and reapplying routes
Explanation	Succeeded to commit IPsec configuration. Flows will be recalculated and reapplied.
Gateway Action	None
Recommended Action	None.

Revision 1

2.22.21. IPsec_successfully_started (ID: 01800202)

Default Severity INFORMATIONAL
Log Message IPsec is up and running
Explanation IPsec configured and started.
Gateway Action None
Recommended Action None.
Revision 1

2.22.22. x509_init_failed (ID: 01800203)

Default Severity CRITICAL
Log Message Failed to initilaze x509 library
Explanation Failed to initilaze x509 library.
Gateway Action IPsec_configuration_disabled
Recommended Action None.
Revision 1

2.22.23. pm_create_failed (ID: 01800204)

Default Severity ERROR
Log Message Failed to create policymanager
Explanation Failed to create policymanager. Out of memory.
Gateway Action reduce_number_of_tunnels
Recommended Action None.
Revision 1

2.22.24. failed_to_start_ipsec (ID: 01800206)

Default Severity ERROR
Log Message Disable all IPsec tunnels
Explanation Disable all IPsec tunnels due to memory limitations.
Gateway Action disable_all_ipsec_interfaces
Recommended Action None.

Revision 1

2.22.25. failed_create_audit_module (ID: 01800207)

Default Severity ERROR
Log Message Failed to create audit module.
Explanation Failed to create audit module.
Gateway Action IPsec_audit_disabled
Recommended Action None.
Revision 1

2.22.26. failed_to_configure_IPsec (ID: 01800210)

Default Severity CRITICAL
Log Message Failed during configuration with error: <error_msg>
Explanation Failed to set IPsec configuration.
Gateway Action IPsec_configuration_disabled
Recommended Action Reconfigure_IPsec.
Revision 1
Parameters error_msg

2.22.27. reconfig_IPsec (ID: 01800211)

Default Severity INFORMATIONAL
Log Message Reconfiguration of IPsec started
Explanation Reconfiguration of IPsec started.
Gateway Action ipsec_reconfigured
Recommended Action None.
Revision 2

2.22.28. IPsec_init_failed (ID: 01800213)

Default Severity CRITICAL
Log Message Failed to initialize IPsec
Explanation Failed to start IPsec.
Gateway Action IPsec_configuration_disabled

Recommended Action	Restart.
Revision	1

2.22.29. ipsec_started_successfully (ID: 01800214)

Default Severity	INFORMATIONAL
Log Message	IPsec started successfully
Explanation	Succeeded to create Policymanger and commit IPsec configuration.
Gateway Action	ipsec_started
Recommended Action	None.
Revision	1

2.22.30. Failed_to_add_certificate (ID: 01800302)

Default Severity	ERROR
Log Message	Failed add host certificate: <certificate>, for tunnel <tunnel>
Explanation	Failed to add specified host certificate.
Gateway Action	certificate_disabled
Recommended Action	Reconfigure_tunnnel.
Revision	1
Parameters	certificate tunnel

2.22.31. Default_IKE_DH_groups_will_be_used (ID: 01800303)

Default Severity	INFORMATIONAL
Log Message	Default configuration for IKE DH groups (2 and 5) will be used for tunnel: <tunnel>
Explanation	Inform that default DH groups settings will be used.
Gateway Action	Use_default_IKE_DH_groups
Recommended Action	None.
Revision	1
Parameters	tunnel

2.22.32. failed_to_set_algorithm_properties (ID: 01800304)

Default Severity	ERROR
Log Message	Failed to set properties IPsec algorithm <alg>, for tunnel <tunnel>
Explanation	Failed to set specified properties (keysize, lifetimes) for IPsec algorithm.
Gateway Action	use_default_values_for_algorithm
Recommended Action	None.
Revision	1
Parameters	alg tunnel

2.22.33. failed_to_set_algorithm_properties (ID: 01800305)

Default Severity	ERROR
Log Message	Failed to set properties for IKE algorithm <alg>, for tunnel <tunnel>
Explanation	Failed to set specified properties (keysize, lifetimes) for IKE algorithm.
Gateway Action	use_default_values_for_algorithm
Recommended Action	None.
Revision	1
Parameters	alg tunnel

2.22.34. failed_to_add_root_certificate (ID: 01800306)

Default Severity	ERROR
Log Message	Failed add root certificate: <certificate>, for tunnel <tunnel>
Explanation	Failed to set specified certificate as root certificate.
Gateway Action	disable_certificate
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	certificate tunnel

2.22.35. dns_resolve_failed (ID: 01800308)

Default Severity	WARNING
Log Message	Failed to resolve remote gateway <gateway> for IPsec Tunnel

	<ipsectunnel>. Keeping old IP <old_ip>
Explanation	Failed to resolve remote gateway through DNS.
Gateway Action	keeping_old_ip
Recommended Action	None.
Revision	1
Parameters	gateway ipsectunnel old_ip

2.22.36. dns_resolve_failed (ID: 01800309)

Default Severity	WARNING
Log Message	Failed to resolve remote gateway <gateway> for IPsec Tunnel <ipsectunnel>. Disabling IPsec tunnel
Explanation	Failed to resolve remote gateway through DNS.
Gateway Action	IPsec_tunnel_disabled
Recommended Action	None.
Revision	1
Parameters	gateway ipsectunnel

2.22.37. failed_to_add_peer (ID: 01800312)

Default Severity	ERROR
Log Message	Failed to add remote gateway: <gateway> resolved by DNS for IPsec tunnel: <ipsectunnel>
Explanation	Failed to add remote gateway, that have been resolved by DNS, to tunnel.
Gateway Action	IPsec_tunnel_disabled
Recommended Action	None.
Revision	1
Parameters	gateway ipsectunnel

2.22.38. failed_to_add_rules (ID: 01800313)

Default Severity	ERROR
Log Message	Failed to add rules after remote gw: <gateway> have been resolved by DNS for IPsec tunnel: <ipsectunnel>

Explanation	Failed to add rules to tunnel after remote gateway have been resolved by DNS.
Gateway Action	IPsec_tunnel_disabled
Recommended Action	None.
Revision	1
Parameters	gateway ipsectunnel

2.22.39. failed_to_add_rules (ID: 01800314)

Default Severity	ERROR
Log Message	Failed to commit rules after remote gw: <gateway> have been resolved by DNS for IPsec tunnel: <ipsectunnel>
Explanation	Failed to add rules to tunnel after remote gateway have been resolved by DNS.
Gateway Action	IPsec_tunnel_disabled
Recommended Action	None.
Revision	1
Parameters	gateway ipsectunnel

2.22.40. new_remote_gw_ip (ID: 01800315)

Default Severity	INFORMATIONAL
Log Message	Resolved remote-gateway <gateway> to IP <ip> for IPsec tunnel <ipsectunnel>
Explanation	Tunnel have succesfully been reconfigured after remote gateway have been resolved.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	gateway ipsectunnel ip

2.22.41. no_policymanager (ID: 01800316)

Default Severity	CRITICAL
Log Message	No policymanager!! to free tunnel object from

Explanation	No policymanager to free tunnel from!!! IPsec does not work properly.
Gateway Action	ipsec_out_of_work
Recommended Action	Restart.
Revision	1

2.22.42. peer_is_dead (ID: 01800317)

Default Severity	INFORMATIONAL
Log Message	Peer <peer> has been detected dead
Explanation	A remote peer have been detected as dead. This will cause all tunnels associated with the peer to be taken down.
Gateway Action	IPsec_tunnel_disabled
Recommended Action	None.
Revision	1
Parameters	peer

2.22.43. failed_to_set_dpdp_cb (ID: 01800318)

Default Severity	ERROR
Log Message	Failed to set callback for Dead Peer Detection
Explanation	Failed to set callback for Dead Peer Detection User will not receive log message when a peer has been detected dead and the tunnel have been killed.
Gateway Action	None
Recommended Action	None.
Revision	1

2.22.44. failed_to_add_key_provider (ID: 01800321)

Default Severity	CRITICAL
Log Message	Failed with error: <status_msg>, when adding external key provider for certificate handling
Explanation	Failed to add external key provider. All certificate authentication will be disabled.
Gateway Action	IPsec_disabled
Recommended Action	Restart.
Revision	1

Parameters status_msg

2.22.45. failed_to_add_certificate (ID: 01800322)

Default Severity	ERROR
Log Message	Failed add certificate: <certificate>, for tunnel <tunnel>
Explanation	Failed to add certificate. Tunnel configured with this certificate for authentication will fail while negotiate.
Gateway Action	certificate_disabled
Recommended Action	None.
Revision	1
Parameters	certificate tunnel

2.22.46. failed_to_set_remote_ID (ID: 01800323)

Default Severity	ERROR
Log Message	Invalid type for ID in remote access idlist: <type>, for tunnel <tunnel>
Explanation	Invalid type for ID in remote access idlist have been specified in configuration.
Gateway Action	vpntunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	type tunnel

2.22.47. failed_to_create_authorization (ID: 01800327)

Default Severity	CRITICAL
Log Message	Failed to create local authorization object
Explanation	Failed to create local authorization object. configured remote access groups will not be possible to use.
Gateway Action	IPsec_disabled
Recommended Action	None.
Revision	1

2.22.48. Failed_to_set_xauth (ID: 01800328)

Default Severity	ERROR
Log Message	Failed set XAuth for tunnel <tunnel>
Explanation	Failed to set extended authentication (XAuth) for the tunnel.
Gateway Action	None
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.22.49. Failed_to_create_xauth_group (ID: 01800329)

Default Severity	CRITICAL
Log Message	Failed create XAuth group
Explanation	Failed to create extended authentication (XAuth) group.
Gateway Action	None
Recommended Action	None.
Revision	1

2.22.50. ippool_does_not_exist (ID: 01800400)

Default Severity	WARNING
Log Message	IP pool does not exist: <ippool>
Explanation	The config mode pool refers to an IP pool that does not exist. As a result, IPsec clients using config mode will not be able lease IP addresses.
Gateway Action	None
Recommended Action	Update your config mode configuration.
Revision	1
Parameters	ippool

2.22.51. cfgmode_ip_freed (ID: 01800402)

Default Severity	NOTICE
Log Message	Returned a dynamic cfg mode IP <ip> to the IP pool
Explanation	A dynamically allocated ip used for IKE cfg mode was returned to the IP pool.
Gateway Action	None

Recommended Action	None.
Revision	1
Parameters	ip

2.22.52. recieved_packet_to_disabled_IPsec (ID: 01800500)

Default Severity	NOTICE
Log Message	received plaintext packet disabled IPsec. Packet will be dropped
Explanation	Received plain text packet to IPsec while disabled.
Gateway Action	packet_will_be_dropped
Recommended Action	None.
Revision	1

2.22.53. recieved_packet_to_disabled_IPsec (ID: 01800501)

Default Severity	NOTICE
Log Message	Received plain text packet to IPsec while shutting down. Packet will be dropped
Explanation	Received plain text packet to IPsec while shutting down.
Gateway Action	packet_will_be_dropped
Recommended Action	None.
Revision	1

2.22.54. Recieved_plaintext_packet_for_disabled_IPsec_interface (ID: 01800502)

Default Severity	WARNING
Log Message	IPsec tunnel <ipsec_connection> is disabled. Packet will be dropped
Explanation	A packed was dropped due to the IPsec interface being disabled.
Gateway Action	packet_will_be_dropped
Recommended Action	This is usually a consequence of low memory or a bad configuration. Look for previous log messages to find the cause for the interface being disabled.
Revision	1
Parameters	ipsec_connection

2.22.55. no_remote_gateway (ID: 01800503)

Default Severity	ERROR
Log Message	Remote gateway is null. No route is possible
Explanation	No remote gateway for packet, i.e no route defined.
Gateway Action	packet_will_be_dropped
Recommended Action	None.
Revision	1

2.22.56. no_route (ID: 01800504)

Default Severity	ERROR
Log Message	Failed to lookup route. No route for packet.
Explanation	No remote gateway for packet, i.e no route defined.
Gateway Action	packet_will_be_dropped
Recommended Action	None.
Revision	1

2.22.57. ping_keepalive_failed_in_tunnel (ID: 01800505)

Default Severity	ERROR
Log Message	IPsec ping monitor detects loss if ping replies of packets INSIDE the tunnel
Explanation	IPsec ping monitor detects loss if ping replies of packets INSIDE the tunnel.
Gateway Action	tunnel_will_disabled_after_8_number_of_lost_packets
Recommended Action	None.
Revision	1

2.22.58. ipsec_interface_disabled (ID: 01800506)

Default Severity	ERROR
Log Message	IPsec interface disabled
Explanation	IPsec interface disabled.
Gateway Action	None
Recommended Action	None.
Revision	1

2.22.59. maximum_allowed_tunnels_limit_reached (ID: 01800900)

Default Severity	ALERT
Log Message	Negotiation aborted due to license restrictions. Reached maximum of <allowed_tunnels> active IPsec tunnels
Explanation	More tunnels and/or unique peers than the license allow are trying to establish.
Gateway Action	negotiation_aborted
Recommended Action	None.
Revision	1
Parameters	allowed_tunnels

2.22.60. SAs_not_killed_for_remote_peer (ID: 01800901)

Default Severity	CRITICAL
Log Message	Failed to kill associated SA:s for <remoteppeer> peer(s)
Explanation	This happens if there is no tunnel established with the given peer.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	remoteppeer

2.22.61. trigger_non_ip_packet (ID: 01802001)

Default Severity	WARNING
Log Message	Trigger for non-IP packet of protocol <proto>. Dropping request for policy
Explanation	Trigger for non IP packet, dropping request.
Gateway Action	dropping_request
Recommended Action	None.
Revision	1
Parameters	proto

2.22.62. rule_not_active (ID: 01802002)

Default Severity	WARNING
Log Message	The rule is not in the active configuration. Dropping request for policy
Explanation	The rule is not in the active configuration, dropping request.
Gateway Action	dropping_request
Recommended Action	None.
Revision	1

2.22.63. malformed_packet (ID: 01802003)

Default Severity	WARNING
Log Message	Malformed packet for trigger.Dropping request for policy
Explanation	Malformed packet for trigger, dropping request.
Gateway Action	dropping_request
Recommended Action	None.
Revision	1

2.22.64. max_ipsec_sa_negotiations_reached (ID: 01802004)

Default Severity	WARNING
Log Message	The maximum number of active Quick-Mode negotiations reached. Rekey not done.
Explanation	Maximum number of active Quick-Mode negotiations reached.
Gateway Action	rekey_not_done
Recommended Action	None.
Revision	1

2.22.65. max_number_of_tunnels_reached (ID: 01802011)

Default Severity	WARNING
Log Message	Negotiation aborted due to license restrictions <maxtunnels>
Explanation	Reached max number of allowed active VPN tunnels according to license.
Gateway Action	ike_negotiation_aborted
Recommended Action	Reconfigure_IPsec.
Revision	1

Parameters	maxtunnels
------------	------------

2.22.66. ike_sa_failed (ID: 01802022)

Default Severity	WARNING
Log Message	Ike SA negotiation failed: <statusmsg> Local IKE peer: <local_peer> Remote IKE peer: <remote_peer> Initiator SPI: <initiator_spi>.
Explanation	Negotiation of IKE SA failed.
Gateway Action	no_ike_sa
Recommended Action	None.
Revision	2
Parameters	statusmsg local_peer remote_peer initiator_spi

2.22.67. ike_sa_negotiation_completed (ID: 01802024)

Default Severity	INFORMATIONAL
Log Message	IKE SA <options> negotiation completed: <mode> using <auth> (<encryption><keysize> - <hash>) Diffie-Hellman group <dhgroup> (<bits>) Lifetime: <lifetime> seconds
Explanation	Negotiation of IKE SA completed.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	options mode auth encryption keysize hash dhgroup bits lifetime

2.22.68. ike_sa_negotiation_failed (ID: 01802030)

Default Severity	INFORMATIONAL
Log Message	No IKE SA negotiations done. Reason: The authentication credentials were not specified or private key was not available
Explanation	No IKE SA negotiations done because of authentication problems.

Gateway Action	no_ike_sa
Recommended Action	None.
Revision	1

2.22.69. ike_sa_negotiation_failed (ID: 01802031)

Default Severity	WARNING
Log Message	Type of the local ID <localid> is not KEY-ID for the mamros-pskeyext negotiation. The negotiation might fail.
Explanation	Type of the local ID is not KEY-ID for the mamros-pskeyext negotiation. The negotiation might fail.
Gateway Action	no_ike_sa
Recommended Action	None.
Revision	1
Parameters	localid

2.22.70. ipsec_sa_negotiation_completed (ID: 01802040)

Default Severity	INFORMATIONAL
Log Message	IPSec SA <sa> <info> negotiation completed:
Explanation	Child SA negotiatiion successfully completed.
Gateway Action	ipsec_sa_enabled
Recommended Action	None.
Revision	2
Parameters	sa info local_peer remote_peer spi_in spi_out [local_ts] [remote_ts]

2.22.71. ipsec_sa_informal (ID: 01802041)

Default Severity	INFORMATIONAL
Log Message	PFS using Diffie-Hellman group: <dhgroup> (<bits>)
Explanation	Information about PFS and Diffie Hellman group used for Child SA.
Gateway Action	None

Recommended Action	None.
Revision	1
Parameters	dhgroup bits

2.22.72. ipsec_sa_informal (ID: 01802043)

Default Severity	INFORMATIONAL
Log Message	Inbound SPI:<spiin> Outbound SPI:<spiout> Algorithm:<alg> <keysize> <mac>
Explanation	Log information about SPI-values and algorithms for Child SA.
Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	spiin spiout alg keysize mac

2.22.73. ipsec_sa_informal (ID: 01802044)

Default Severity	INFORMATIONAL
Log Message	Inbound SPI:<spiin> Outbound SPI:<spiout> Algorith:<mac>
Explanation	Log information about SPI-values and algorithms fro Child SA.
Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	spiin spiout mac

2.22.74. ipsec_sa_lifetime (ID: 01802045)

Default Severity	INFORMATIONAL
Log Message	Local lifetime child SA: <kb> kilobytes, <sec> seconds
Explanation	Inform about lifetime for child SA:.
Gateway Action	None
Recommended Action	None.

Revision	1
Parameters	kb sec

2.22.75. ipsec_sa_lifetime (ID: 01802046)

Default Severity	INFORMATIONAL
Log Message	Local lifetime child SA: <sec> seconds
Explanation	Inform about lifetime for child SA:.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	sec

2.22.76. ipsec_sa_lifetime (ID: 01802047)

Default Severity	INFORMATIONAL
Log Message	Local lifetime child SA: <kb> kilobytes
Explanation	Inform about lifetime for child SA:.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	kb

2.22.77. ipsec_sa_lifetime (ID: 01802048)

Default Severity	INFORMATIONAL
Log Message	Local lifetime child SA: infinite
Explanation	Inform about lifetime for child SA.
Gateway Action	None
Recommended Action	None.
Revision	1

2.22.78. ipsec_sa_informal (ID: 01802058)

Default Severity	INFORMATIONAL
-------------------------	---------------

Log Message	Local Proxy ID: <local_id>, Remote Proxy ID: <remote_id>
Explanation	Information about Proxy ID's for Child SA.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	local_id remote_id

2.22.79. ipsec_invalid_protocol (ID: 01802059)

Default Severity	ERROR
Log Message	Invalid protocol <proto> received for SA
Explanation	Invalid protocol received for SA.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	proto

2.22.80. ipsec_sa_negotiation_aborted (ID: 01802060)

Default Severity	ERROR
Log Message	IPsec SA Negotiation aborted: AH can not be initiated with NAT-T
Explanation	Negotiation aborted since AH can not be initiated with NAT-T.
Gateway Action	ipsec_sa_negotiation_aborted
Recommended Action	None.
Revision	1

2.22.81. create_rules_failed (ID: 01802080)

Default Severity	ERROR
Log Message	Cannot insert this rule, the forced NAT protocol type does not match rule protocol
Explanation	Failed to insert rule since forced NAT protocol do not match rule protocol.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.

Revision 1

2.22.82. create_rules_failed (ID: 01802081)

Default Severity	ERROR
Log Message	Cannot insert this rule, the forced NAT protocol type does not match rule protocol
Explanation	Failed to insert rule since forced NAT protocol do not match rule protocol.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.22.83. no_authentication_method_specified (ID: 01802100)

Default Severity	ERROR
Log Message	Neither pre-shared keys nor CA certificates nor EAP are specified for a tunnel
Explanation	No authentication method is specified for the tunnel.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.22.84. no_key_method_configured_for_tunnel (ID: 01802102)

Default Severity	ERROR
Log Message	Tunnel does not specify any keying method (IKE or manual)
Explanation	No keying method (IKE/manual) is configured for tunnel.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.22.85. invalid_configuration_of_force_open (ID: 01802104)

Default Severity	ERROR
Log Message	Auto-start rule does not specify single IP address or domain name for its remote peer
Explanation	Can not use Auto-start rule (force open) for roaming tunnels.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_IPsec.
Revision	1

2.22.86. invalid_rule_setting (ID: 01802105)

Default Severity	ERROR
Log Message	Both REJECT and PASS defined for a rule
Explanation	Can not specify both pass and reject for a rule.
Gateway Action	None
Recommended Action	None.
Revision	1

2.22.87. invalid_rule_setting (ID: 01802106)

Default Severity	ERROR
Log Message	The AUTHENTICATION-ONLY can be specified only for PASS rules
Explanation	Can only specify AUTHENTICATION-ONLY with PASS rules.
Gateway Action	None
Recommended Action	None.
Revision	1

2.22.88. invalid_rule_setting (ID: 01802107)

Default Severity	ERROR
Log Message	To-tunnel specified for a REJECT rule
Explanation	To-tunnel can not be specified for REJECT rule.
Gateway Action	None
Recommended Action	None.
Revision	1

2.22.89. invalid_rule_setting (ID: 01802108)

Default Severity	ERROR
Log Message	No from-tunnel specified for an AUTHENTICATION-ONLY rule
Explanation	From-tunnel must be specified for an AUTHENTICATION-ONLY rule.
Gateway Action	None
Recommended Action	None.
Revision	1

2.22.90. invalid_rule_setting (ID: 01802109)

Default Severity	ERROR
Log Message	To-tunnel specified for an AUTHENTICATION-ONLY rule
Explanation	To-tunnel can not be specified for an AUTHENTICATION-ONLY rule.
Gateway Action	None
Recommended Action	None.
Revision	1

2.22.91. max_number_of_policy_rules_reached (ID: 01802110)

Default Severity	CRITICAL
Log Message	The maximum number of policy rules reached
Explanation	The maximum number of policy rules reached.
Gateway Action	VPN_configuration_disabled
Recommended Action	Reconfig.
Revision	1

2.22.92. suspicious_outbound_rule (ID: 01802114)

Default Severity	ERROR
Log Message	Detected suspicious outbound IPSec rule without any selectors
Explanation	Detected suspicious outbound IPSec rule without any selectors specified.
Gateway Action	the_rule_might_not_work

Recommended Action	Reconfigure_IPSec.
Revision	1

2.22.93. no_algorithms_configured_for_tunnel (ID: 01802200)

Default Severity	ERROR
Log Message	ESP tunnel is missing encryption and authentication algorithms
Explanation	ESP tunnel [tunnel] not configured with encryption and authentication algorithms.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.22.94. no_encryption_algorithm_configured_for_tunnel (ID: 01802201)

Default Severity	ERROR
Log Message	ESP tunnel <tunnel> is missing encryption algorithm. Null encryption algorithm must be specified if no encryption is required
Explanation	ESP tunnel not configured with any encryption algorithm, not even Null.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.22.95. no_authentication_algorithm_specified (ID: 01802203)

Default Severity	ERROR
Log Message	No authentication algorithm configured for AH tunnel <tunnel>
Explanation	AH tunnel is configured without spetication algorithm.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1

Parameters	tunnel
------------	--------

2.22.96. AH_not_supported (ID: 01802204)

Default Severity	ERROR
Log Message	AH configured but not supported
Explanation	Tunnel [tunnel] configured for AH, but AH is not supported.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.22.97. invalid_tunnel_configuration (ID: 01802208)

Default Severity	ERROR
Log Message	No IPSec transform (AH or ESP) specified for tunnel <tunnel>
Explanation	IPSec transform type must be specified for tunnel.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.22.98. invalid_tunnel_configuration (ID: 01802209)

Default Severity	ERROR
Log Message	Auto-start tunnel <tunnel> configured for `per-port' or `per-host' SA.
Explanation	`per-port' or `per-host' SA can not be specified for auto-start tunnels [tunnel].
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.22.99. invalid_tunnel_configuration (ID: 01802210)

Default Severity	ERROR
------------------	-------

Log Message	Both `auto-start' and `dont-initiate' specified for tunnel <tunnel>
Explanation	Both `auto-start' and `dont-initiate' can not be specified for a tunnel.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	tunnel

2.22.100. out_of_memory_for_tunnel (ID: 01802211)

Default Severity	ERROR
Log Message	Out of memory. Could not allocate memory for tunnel name! <tunnel>
Explanation	Out of memory. Could not allocate memory for tunnel name!.
Gateway Action	VPN_tunnel_disabled
Recommended Action	None.
Revision	1
Parameters	tunnel

2.22.101. invalid_key_size (ID: 01802214)

Default Severity	ERROR
Log Message	Invalid key sizes specified for algorithms
Explanation	Invalid key sizes specified for algorithms.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2

2.22.102. invalid_key_size (ID: 01802215)

Default Severity	ERROR
Log Message	Algorithm key sizes specified for unknown algorithm
Explanation	Algorithm key sizes specified for unknown algorithm.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2

2.22.103. invalid_key_size (ID: 01802216)

Default Severity	ERROR
Log Message	Algorithm key sizes specified for unknown algorithm
Explanation	Algorithm key sizes specified for unknown algorithm.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2

2.22.104. invalid_key_size (ID: 01802217)

Default Severity	ERROR
Log Message	Specified key size limits for cipher <alg> with fixed key size
Explanation	Configuration specifies key size limits for cipher with fixed key size.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	2
Parameters	alg

2.22.105. invalid_cipher_keysize (ID: 01802218)

Default Severity	ERROR
Log Message	Configured max cipher key size <keysize> is bigger than the built-in maximum <max>
Explanation	Tunnel configured invalid key size for cipher.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	keysize max

2.22.106. invalid_key_size (ID: 01802219)

Default Severity	ERROR
Log Message	Tunnel specified key size limits for mac <alg> with fixed key size
Explanation	Configuration specifies key size limits for cipher with fixed key size.

Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	alg

2.22.107. invalid_cipher_keysize (ID: 01802220)

Default Severity	ERROR
Log Message	Configured max MAC key size <keysize> is bigger than the built-in maximum <max>
Explanation	Tunnel configured invalid key size for MAC.
Gateway Action	VPN_tunnel_disabled
Recommended Action	Reconfigure_tunnel.
Revision	1
Parameters	keysize max

2.22.108. malformed_tunnel_id_configured (ID: 01802225)

Default Severity	ERROR
Log Message	Malformed identity <id> configured for tunnel
Explanation	Malformed identity specified in configuration.
Gateway Action	VPN_tunnel_invalid
Recommended Action	Reconfigure_remote_id.
Revision	1
Parameters	id

2.22.109. malformed_psk_configured (ID: 01802229)

Default Severity	ERROR
Log Message	Malformed IKE secret (PSK) configured for tunnel
Explanation	Malformed IKE secret specified in configuration.
Gateway Action	VPN_tunnel_invalid
Recommended Action	Reconfigure_PSK.
Revision	1

2.22.110. rule_selection_failed (ID: 01802300)

Default Severity	NOTICE
Log Message	Rule selection failed: <info>. Internal severity level: <int_severity>
Explanation	Rule selection failed!.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	info int_severity

2.22.111. max_phase1_sa_reached (ID: 01802400)

Default Severity	NOTICE
Log Message	The maximum number of active Phase-1 SAs reached
Explanation	Maximum number of active Phase-1 SAs reached.
Gateway Action	negotiation_aborted
Recommended Action	None.
Revision	1

2.22.112. max_phase1_negotiations_reached (ID: 01802402)

Default Severity	NOTICE
Log Message	The maximum number of active Phase-1 negotiations reached
Explanation	Maximum number of active Phase-1 negotiations reached.
Gateway Action	negotiation_aborted
Recommended Action	None.
Revision	2

2.22.113. max_active_quickmode_negotiation_reached (ID: 01802403)

Default Severity	NOTICE
Log Message	The maximum number of active Quick-Mode negotiations reached
Explanation	Maximum number of active Quick-Mode negotiations reached.

Gateway Action	quick-mode_not_done
Recommended Action	None.
Revision	1

2.22.114. could_not_decode_certificate (ID: 01802600)

Default Severity	WARNING
Log Message	Could not decode Certificate to pem format. The certificate may be corrupted or it was given in unrecognized format.
Explanation	Could_not_decode_certificate.
Gateway Action	certificate_invalid
Recommended Action	None.
Revision	1

2.22.115. could_not_convert_certificate (ID: 01802601)

Default Severity	WARNING
Log Message	Could not convert CMi certificate to X.509 certificate
Explanation	Could not convert CMi certificate to X.509 certificate.
Gateway Action	certificate_invalid
Recommended Action	None.
Revision	1

2.22.116. could_not_get_subject_name_from_ca_cert (ID: 01802602)

Default Severity	WARNING
Log Message	Could not get subject name from a CA certificate. This certificate is not usable as an IPsec authenticator, and is not inserted into local list of trusted CAs
Explanation	Could not get subject name from a CA certificate.
Gateway Action	certificate_not_trusted
Recommended Action	None.
Revision	1

2.22.117. could_not_set_cert_to_non_CRL_issuer (ID: 01802603)

Default Severity	WARNING
Log Message	Could not set CA certificate to non-CRL issuer. This may cause authentication errors if valid CRLs are not available
Explanation	Could not set CA certificate to non-CRL issuer.
Gateway Action	certificate_not_usable_if_no_valid_CRLs
Recommended Action	None.
Revision	1

2.22.118. could_not_force_cert_to_be_trusted (ID: 01802604)

Default Severity	WARNING
Log Message	Could not force CA certificate as a point of trust
Explanation	Could not force CA certificate as a point of trust.
Gateway Action	certificate_disabled
Recommended Action	None.
Revision	1

2.22.119. could_not_trusted_set_for_cert (ID: 01802605)

Default Severity	WARNING
Log Message	Could not set the trusted set for a CA certificate
Explanation	Could not set the trusted set for a CA certificate.
Gateway Action	certificate_disabled
Recommended Action	None.
Revision	1

2.22.120. could_not_insert_cert_to_db (ID: 01802606)

Default Severity	ERROR
Log Message	Can not insert CA certificate into local database
Explanation	Can not insert CA certificate into local database.
Gateway Action	certificate_disabled
Recommended Action	None.
Revision	1

2.22.121. could_not_decode_certificate (ID: 01802607)

Default Severity	WARNING
Log Message	Could not decode Certificate to pem format. The certificate may be corrupted or it was given in unrecognized format.
Explanation	Could_not_decode_certificate.
Gateway Action	certificate_invalid
Recommended Action	None.
Revision	1

2.22.122. could_not_lock_certificate (ID: 01802608)

Default Severity	WARNING
Log Message	Could not lock certificate in cache
Explanation	Could not lock certificate in cache.
Gateway Action	certificate_invalid
Recommended Action	None.
Revision	1

2.22.123. could_not_insert_cert_to_db (ID: 01802609)

Default Severity	ERROR
Log Message	Could not insert certificate into local database
Explanation	Could not insert certificate into local database.
Gateway Action	certificate_disabled
Recommended Action	None.
Revision	1

2.22.124. could_not_decode_crl (ID: 01802610)

Default Severity	WARNING
Log Message	Could not decode CRL. The certificate may be corrupted or it was given in unrecognized format. File format may be wrong
Explanation	Could_not_decode_CRL.
Gateway Action	certificate_invalid
Recommended Action	None.

Revision 1

2.22.125. ike_sa_negotiation_completed (ID: 01802703)

Default Severity	INFORMATIONAL
Log Message	IKE SA: Local IKE peer: <local_peer> Remote IKE peer: <remote_peer> Initiator SPI: <initiator_spi> Responder SPI: <responder_spi>. Internal severity level: <int_severity>.
Explanation	Ike SA successfully installed.
Gateway Action	ike_sa_completed
Recommended Action	None.
Revision	1
Parameters	local_peer remote_peer initiator_spi responder_spi int_severity

2.22.126. ike_sa_negotiation_completed (ID: 01802704)

Default Severity	INFORMATIONAL
Log Message	IKE SA: Local IKE peer: <local_peer> Remote IKE peer: <remote_peer>. Internal severity level: <int_severity>
Explanation	Ike SA successfully installed.
Gateway Action	ike_sa_completed
Recommended Action	None.
Revision	1
Parameters	local_peer remote_peer int_severity

2.22.127. Certificate_contains_bad_IP_address (ID: 01802705)

Default Severity	WARNING
Log Message	Certificate contains bad IP address: length=<len>
Explanation	Certificate contains bad IP address.
Gateway Action	try_next_certificate
Recommended Action	None.

Revision	1
Parameters	len

2.22.128. dn_name_as_subject_alt_name (ID: 01802706)

Default Severity	WARNING
Log Message	Directory names are not supported as subject alternative names. Skipping DN: <dn_name>
Explanation	Directory specified as subject alternative name.
Gateway Action	skip_dn_name
Recommended Action	None.
Revision	1
Parameters	dn_name

2.22.129. could_not_decode_certificate (ID: 01802707)

Default Severity	WARNING
Log Message	Could not decode Certificate to pem format. The certificate may be corrupted or it was given in unrecognized format.
Explanation	Could_not_decode_certificate.
Gateway Action	certificate_invalid
Recommended Action	None.
Revision	1

2.22.130. ike_sa_destroyed (ID: 01802708)

Default Severity	INFORMATIONAL
Log Message	IKE SA destroyed: <ike_sa>
Explanation	Ike SA is destroyed.
Gateway Action	ike_sa_killed
Recommended Action	None.
Revision	1
Parameters	ike_sa

2.22.131. cfgmode_exchange_event (ID: 01802709)

Default Severity	INFORMATIONAL
Log Message	Event occurred for config mode <cfgmode> exchange: <msg>. Internal severity level: <int_severity>
Explanation	Config mode exchange event.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	cfgmode msg int_severity

2.22.132. remote_access_address (ID: 01802710)

Default Severity	INFORMATIONAL
Log Message	Addresses for remote access attributes: <ipaddr> expires time <time>
Explanation	Addresses for remote access attributes.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	ipaddr [time]

2.22.133. remote_access_dns (ID: 01802711)

Default Severity	INFORMATIONAL
Log Message	DNS for remote access attributes: <dns_server>
Explanation	DNS for remote access attributes.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	dns_server

2.22.134. remote_access_wins (ID: 01802712)

Default Severity	INFORMATIONAL
Log Message	WINS for remote access attributes: <win>
Explanation	WINS for remote access attributes.

Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	win

2.22.135. remote_access_dhcp (ID: 01802713)

Default Severity	INFORMATIONAL
Log Message	DHCP for remote access attributes: <dhcp_s>
Explanation	DHCP remote access attributes.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	dhcp_s

2.22.136. remote_access_subnets (ID: 01802714)

Default Severity	INFORMATIONAL
Log Message	Subnets remote access attributes: <subnets>
Explanation	Subnets remote access attributes.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	subnets

2.22.137. event_on_ike_sa (ID: 01802715)

Default Severity	WARNING
Log Message	Event: <msg> occurred for IKE SA: <side>. Internal severity level: <int_severity>
Explanation	Event occurred at IKE SA.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	side msg

int_severity

2.22.138. ipsec_sa_selection_failed (ID: 01802717)

Default Severity	WARNING
Log Message	Selection of IPSec SA failed due to <reason>. Internal severity level: <int_severity>
Explanation	Failed to select a SA.
Gateway Action	no_ipsec_sa_selected
Recommended Action	None.
Revision	1
Parameters	reason int_severity

2.22.139. certificate_search_failed (ID: 01802718)

Default Severity	WARNING
Log Message	Certificate manager search failure: <reason>. Internal severity level: <int_severity>
Explanation	Search for matching certificate failed.
Gateway Action	certificate_failure
Recommended Action	None.
Revision	1
Parameters	reason int_severity

2.22.140. ipsec_sa_event (ID: 01802730)

Default Severity	WARNING
Log Message	IPSec SA negotiation event: <msg>, <local_proxy>, <remote_proxy>. Internal severity level: <int_severity>
Explanation	Event occurred for IPSec SA.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	msg local_proxy remote_proxy int_severity

2.22.141. ipsec_sa_event (ID: 01802731)

Default Severity	WARNING
Log Message	IPSec SA negotiation event: <msg>. Internal severity level: <int_severity>
Explanation	Event occurred for IPSec SA.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	msg int_severity

2.22.142. ipsec_sa_destroyed (ID: 01802732)

Default Severity	INFORMATIONAL
Log Message	IPSec SA destroyed: Inbound SPI: <spiin> Outbound SPI: <spiout>
Explanation	IPSec SA have been destroyed.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	spiin spiout

2.22.143. (ID: 01802735)

Default Severity	INFORMATIONAL
Log Message	L2TP <side> negotiation event: <msg>. <local_peer>, <remote_peer>. Internal severity level: <int_severity>
Explanation	L2TP negotiation event.
Gateway Action	l2tp_negotiation_event
Recommended Action	None.
Revision	1
Parameters	side msg local_peer remote_peer int_severity

2.22.144. (ID: 01802736)

Default Severity	INFORMATIONAL
Log Message	L2TP <side> negotiation event: <msg>. <local_id>, <remote_id>. Internal severity level: <int_severity>
Explanation	L2TP negotiation event.
Gateway Action	l2tp_negotiation_event
Recommended Action	None.
Revision	1
Parameters	side msg local_id remote_id int_severity

2.22.145. outofmem_create_engine (ID: 01802901)

Default Severity	CRITICAL
Log Message	Failed to allocate memory for engine object
Explanation	Could not allocate memory for engine object.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.146. init_rulelookup_failed (ID: 01802903)

Default Severity	CRITICAL
Log Message	Initialization of rule lookup failed
Explanation	Initialization of rule lookup failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.147. init_rule_lookup_failed (ID: 01802904)

Default Severity	CRITICAL
Log Message	Allocating default drop rule failed!
Explanation	Allocating default drop rule failed!.

Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.148. init_rule_lookup_failed (ID: 01802905)

Default Severity	CRITICAL
Log Message	allocating default pass rule failed!
Explanation	Allocating default pass rule failed!.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.149. init_mutexes_failed (ID: 01802906)

Default Severity	CRITICAL
Log Message	Allocating mutexes failed
Explanation	Allocating mutexes failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.150. init_interface_table_failed (ID: 01802907)

Default Severity	CRITICAL
Log Message	Initialization of interface table failed
Explanation	Initialization of interface table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.151. init_flow_id_table_failed (ID: 01802908)

Default Severity	CRITICAL
Log Message	Allocation of flow id hash tables failed
Explanation	Allocation of flow id hash tables failed.

Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.152. init_flow_table_failed (ID: 01802909)

Default Severity	CRITICAL
Log Message	Allocation of flow table failed (size <size>)
Explanation	Allocation of flow table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1
Parameters	size

2.22.153. init_next_hop_table_failed (ID: 01802910)

Default Severity	CRITICAL
Log Message	Allocation of next hop table failed
Explanation	Allocation of next hop table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.154. init_transform_table_failed (ID: 01802911)

Default Severity	CRITICAL
Log Message	Allocation of transform table failed (size <size>)
Explanation	Allocation of transform table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1
Parameters	size

2.22.155. init_peer_hash_failed (ID: 01802912)

Default Severity	CRITICAL
-------------------------	----------

Log Message	Allocation of peer hash table failed
Explanation	Allocation of peer hash table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.156. init_peer_id_hash_failed (ID: 01802913)

Default Severity	CRITICAL
Log Message	Allocation of peer id hash table failed
Explanation	Allocation of peer id hash table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.157. init_rule_table_failed (ID: 01802914)

Default Severity	CRITICAL
Log Message	Allocation of rule table failed
Explanation	Allocation of rule table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.158. init_inbound_spi_hash_failed (ID: 01802915)

Default Severity	CRITICAL
Log Message	Allocation of inbound spi hash table failed
Explanation	Allocation of inbound spi hash table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.159. init_transform_context_hash_failed (ID: 01802916)

Default Severity	CRITICAL
Log Message	Allocation of transform context hash table failed
Explanation	Allocation of transform context hash table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.160. init_packet_context_cache_failed (ID: 01802917)

Default Severity	CRITICAL
Log Message	Allocation of packet context cache failed
Explanation	Allocation of packet context cache failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.161. init_transform_context_table_failed (ID: 01802918)

Default Severity	CRITICAL
Log Message	Allocation of transform context table failed
Explanation	Allocation of transform context table failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.162. init_nat_table_failed (ID: 01802919)

Default Severity	CRITICAL
Log Message	Allocation of NAT tables failed
Explanation	Allocation of NAT tables failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.163. init_frag_table_failed (ID: 01802920)

Default Severity	CRITICAL
Log Message	Allocation of fragmentation tables failed
Explanation	Allocation of fragmentation tables failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.164. init_engine_tables_failed (ID: 01802921)

Default Severity	CRITICAL
Log Message	Allocation of engine tables failed
Explanation	Allocation of engine tables failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.165. init_interceptor_failed (ID: 01802922)

Default Severity	CRITICAL
Log Message	Opening the interceptor failed
Explanation	Opening the interceptor failed.
Gateway Action	ipsec_disabled
Recommended Action	None.
Revision	1

2.22.166. malformed_ike_sa_proposal (ID: 01803000)

Default Severity	WARNING
Log Message	Malformed IKE SA proposal: <reason>
Explanation	Received a malformed IKE SA proposal.
Gateway Action	None
Recommended Action	None.
Revision	1

Parameters reason

2.22.167. failed_to_select_policy_rule (ID: 01803001)

Default Severity INFORMATIONAL
Log Message Could not select policy rule
Explanation Could not select policy rule.
Gateway Action None
Recommended Action None.
Revision 1

2.22.168. failed_to_select_ike_sa (ID: 01803002)

Default Severity INFORMATIONAL
Log Message Could not select SA from IKE SA proposal
Explanation Could not select SA from IKE SA proposal.
Gateway Action None
Recommended Action None.
Revision 1

2.22.169. ike_phase1_notification (ID: 01803003)

Default Severity WARNING
Log Message <status> Phase-1 notification from <remote_peer> for protocol
<proto>, SPI <spi>: <msg> (<type>) (<size> bytes)
Explanation Received a IKE Phase-2 notification.
Gateway Action None
Recommended Action None.
Revision 1
Parameters status
 remote_peer
 proto
 spi
 msg
 type
 size

2.22.170. ipsec_sa_failed (ID: 01803020)

Default Severity	WARNING
Log Message	IPsec SA negotiation failed: <statusmsg>
Explanation	Negotiation of IPsec SA failed.
Gateway Action	no_ipsec_sa
Recommended Action	None.
Revision	1
Parameters	statusmsg

2.22.171. ipsec_sa_statistics (ID: 01803021)

Default Severity	INFORMATIONAL
Log Message	IPsec SA negotiations: <done> done, <success> successful, <failed> failed
Explanation	IPsec SA statistics.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	done success failed

2.22.172. config_mode_exchange_event (ID: 01803022)

Default Severity	INFORMATIONAL
Log Message	Config Mode exchange event: <msg>. <reason>.
Explanation	A Config Mode exchange event occurred.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	msg reason

2.22.173. config_mode_exchange_event (ID: 01803023)

Default Severity	INFORMATIONAL
Log Message	Config Mode exchange event: <msg>.

Explanation	A Config Mode exchange event occurred.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	msg

2.22.174. xauth_exchange_done (ID: 01803024)

Default Severity	INFORMATIONAL
Log Message	XAuth exchange done: <statusmsg>
Explanation	Information about the result of a completed XAuth exchange.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	statusmsg

2.22.175. config_mode_exchange_event (ID: 01803025)

Default Severity	INFORMATIONAL
Log Message	Config Mode exchange event: <msg>. <reason>.
Explanation	A Config Mode exchange event occurred.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	msg reason

2.22.176. config_mode_exchange_event (ID: 01803026)

Default Severity	INFORMATIONAL
Log Message	Config Mode exchange event: <msg>.
Explanation	A Config Mode exchange event occurred.
Gateway Action	None
Recommended Action	None.
Revision	1

Parameters	msg
------------	-----

2.22.177. rejecting_ipsec_sa_delete (ID: 01803027)

Default Severity	WARNING
Log Message	Rejecting IPsec SA delete notification from <remote_peer> since it was for protocol <proto>
Explanation	Rejected IPsec SA delete notification due to protocol mismatch.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	remote_peer proto

2.22.178. rejecting_ipsec_sa_delete (ID: 01803028)

Default Severity	WARNING
Log Message	Rejecting IPsec SA delete notification from <remote_peer> since the SPI size <spi_size> does not match the expected value 4
Explanation	Rejected IPsec SA delete notification because the SPI size did not match the expected value 4.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	remote_peer spi_size

2.22.179. ike_phase2_notification (ID: 01803029)

Default Severity	WARNING
Log Message	<status> Phase-2 notification from <remote_peer> for protocol <proto>, SPI <spi>: <msg> (<type>) (<size> bytes)
Explanation	Received a IKE Phase-2 notification.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	status remote_peer proto

spi
msg
type
size

2.22.180. ike_qm_notification (ID: 01803030)

Default Severity	WARNING
Log Message	Quick-Mode notification from <remote_peer> for protocol <proto>, SPI <spi>: <msg> (<type>) (<size> bytes)
Explanation	Received a IKE Quick-Mode notification.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	remote_peer proto spi msg type size

2.22.181. failed_to_verify_peer_identity (ID: 01803040)

Default Severity	INFORMATIONAL
Log Message	Could not verify remote peer's identity
Explanation	Could not verify remote peer's identity.
Gateway Action	None
Recommended Action	None.
Revision	1

2.22.182. malformed_ipsec_sa_proposal (ID: 01803050)

Default Severity	WARNING
Log Message	Malformed IPsec SA proposal: <reason>
Explanation	Received a malformed IPsec SA proposal.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.22.183. malformed_ipsec_esp_proposal (ID: 01803051)

Default Severity	WARNING
Log Message	Malformed IPsec ESP proposal: <reason>
Explanation	Received a malformed IPsec ESP proposal.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.22.184. malformed_ipsec_ah_proposal (ID: 01803052)

Default Severity	WARNING
Log Message	Malformed IPsec AH proposal: <reason>
Explanation	Received a malformed IPsec AH proposal.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.22.185. failed_to_select_ipsec_proposal (ID: 01803053)

Default Severity	WARNING
Log Message	Could not select proposal for IPsec SA <sa_index>
Explanation	Could not select proposal for IPsec SA.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	sa_index

2.22.186. failed_to_select_ipsec_sa (ID: 01803054)

Default Severity	INFORMATIONAL
Log Message	Could not select SA from IPsec SA proposal
Explanation	Could not select SA from IPsec SA proposal.

Gateway Action	None
Recommended Action	None.
Revision	1

2.22.187. ike_responder_mode_not_available (ID: 01803101)

Default Severity	NOTICE
Log Message	Negotiation aborted due to license restrictions: IKE responder mode not available.
Explanation	A negotiation was aborted because it was not initiated by the correct side in accordance with license restrictions.
Gateway Action	ike_negotiation_aborted
Recommended Action	None.
Revision	1

2.22.188. audit_event (ID: 01803200)

Default Severity	INFORMATIONAL
Log Message	An audit event occurred: <msg>. Internal severity level: <int_severity>
Explanation	An audit event occurred in the IPsec stack.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	msg int_severity

2.22.189. failed_to_find_userauthobject_for_ipsec_sa (ID: 01803302)

Default Severity	NOTICE
Log Message	No userauth object were found for IP <cfgmodeip> on iface <iface>. The IPsec SA will not be imported.
Explanation	Failed to find an userauth object when importing a IPsec SA. The IPsec SA will not be imported.
Gateway Action	None
Recommended Action	None.

Revision	1
Parameters	cfgmodeip iface

2.23. IP_ERROR

These log messages refer to the **IP_ERROR (Packet discarded due to IP header error(s))** category.

2.23.1. too_small_packet (ID: 01500001)

Default Severity	WARNING
Log Message	Packet is too small to contain IPv4 header
Explanation	The received packet is too small to contain an IPv4 header, and will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.23.2. disallowed_ip_ver (ID: 01500002)

Default Severity	WARNING
Log Message	Disallowed IP version <ipver>
Explanation	The received packet has a disallowed IP version, and will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipver
Context Parameters	Rule Name Packet Buffer

2.23.3. invalid_ip_length (ID: 01500003)

Default Severity	WARNING
Log Message	Invalid IP header length - IPTotLen=<iptotlen>, IPHdrLen=<iphdrLen>
Explanation	The received packet IP header specifies an invalid length. The IP Header length can never be smaller than 20 bytes or longer than the total packet length. Dropping packet.
Gateway Action	drop
Recommended Action	None.

Revision	1
Parameters	iptotlen iphdrln
Context Parameters	Rule Name Packet Buffer

2.23.4. invalid_ip_length (ID: 01500004)

Default Severity	WARNING
Log Message	Invalid IP header length, IPTotLen=<iptotlen>, RecvLen=<recvlen>
Explanation	The received packet IP total length is larger than the received transport data. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	iptotlen recvlen
Context Parameters	Rule Name Packet Buffer

2.23.5. invalid_ip_checksum (ID: 01500005)

Default Severity	WARNING
Log Message	Invalid IP header checksum - RecvChkSum=<recvchksum>, CompChkSum=<compchksum>
Explanation	The received packet IP header checksum is invalid, dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	recvchksum compchksum
Context Parameters	Rule Name Packet Buffer

2.24. IP_FLAG

These log messages refer to the **IP_FLAG (Events concerning the IP header flags)** category.

2.24.1. ttl_low (ID: 01600001)

Default Severity	WARNING
Log Message	Received packet with too low TTL of <ttl>. Min TTL is <ttlmin>. Ignoring
Explanation	The received packet has a TTL (Time-To-Live) field which is too low. Ignoring and forwarding packet anyway.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	ttl ttlmin
Context Parameters	Rule Name Packet Buffer

2.24.2. ip_rsv_flag_set (ID: 01600002)

Default Severity	NOTICE
Log Message	The IP Reserved Flag was set. Ignoring
Explanation	The received packet has the IP Reserved Flag set. This is ignored.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.24.3. ip_rsv_flag_set (ID: 01600003)

Default Severity	WARNING
Log Message	The IP Reserved Flag was set, stripping
Explanation	The received packet has the IP Reserved Flag set. Removing it.
Gateway Action	strip_flag
Recommended Action	None.
Revision	1

Context Parameters	Rule Name
	Packet Buffer

2.25. IP_OPT

These log messages refer to the **IP_OPT (Events concerning the IP header options)** category.

2.25.1. source_route (ID: 01700001)

Default Severity	NOTICE
Log Message	Packet has a source route
Explanation	The packet has a source route. Ignoring.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.25.2. timestamp (ID: 01700002)

Default Severity	NOTICE
Log Message	Packet has a timestamp IP Option
Explanation	The packet contains a timestamp IP Option. Ignoring.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.25.3. router_alert (ID: 01700003)

Default Severity	NOTICE
Log Message	Packet has a router alert IP option
Explanation	The packet contains a router alert IP Option. Ignoring.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.25.4. ipopt_present (ID: 01700004)

Default Severity	NOTICE
Log Message	IP Option <ipopt>(<optname>) is present
Explanation	The packet contains an IP Option. Ignoring.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	ipopt optname
Context Parameters	Rule Name Packet Buffer

2.25.5. ipoptlen_too_small (ID: 01700010)

Default Severity	WARNING
Log Message	Type <ipopt> is multibyte, available <avail>. Dropping
Explanation	The IP Option type is multi byte which requires two bytes, and there is less than two bytes available. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt minoptlen avail
Context Parameters	Rule Name Packet Buffer

2.25.6. ipoptlen_invalid (ID: 01700011)

Default Severity	WARNING
Log Message	Type <ipopt> claims len=<optlen>, available=<avail>. Dropping
Explanation	The IP Option type does not fit in the option space. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt optlen

	avail
Context Parameters	Rule Name Packet Buffer

2.25.7. multiple_ip_option_routes (ID: 01700012)

Default Severity	WARNING
Log Message	Multiple source/return routes in IP options. Dropping
Explanation	There are multiple source/return routes specified among the IP Options. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.25.8. bad_length (ID: 01700013)

Default Severity	WARNING
Log Message	IP Option Type <ipopt>: Bad length <optlen> for <route> Route. Dropping
Explanation	An invalid length is specified for the IP Option type. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt optlen route
Context Parameters	Rule Name Packet Buffer

2.25.9. bad_route_pointer (ID: 01700014)

Default Severity	WARNING
Log Message	IP Option Type <ipopt>: Bad Source Route Pointer <routeptr>. Dropping
Explanation	The packet has a Source Route Pointer, which is invalid. Dropping packet.
Gateway Action	drop

Recommended Action	None.
Revision	1
Parameters	ipopt routepr
Context Parameters	Rule Name Packet Buffer

2.25.10. source_route_disallowed (ID: 01700015)

Default Severity	WARNING
Log Message	Source route IP option disallowed. Dropping
Explanation	The packet has a source route, which is disallowed. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.25.11. multiple_ip_option_timestamps (ID: 01700016)

Default Severity	WARNING
Log Message	Multiple timestamps in IP options. Dropping
Explanation	The packet contains mutiple timestamps in IP Options. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.25.12. bad_timestamp_len (ID: 01700017)

Default Severity	WARNING
Log Message	IP Option Type <ipopt>: Bad length <optlen>. Dropping
Explanation	The packet contains an IP Option, which has an invalid lenth. Dropping packet.
Gateway Action	drop
Recommended Action	None.

Revision	1
Parameters	ipopt optlen
Context Parameters	Rule Name Packet Buffer

2.25.13. bad_timestamp_pointer (ID: 01700018)

Default Severity	WARNING
Log Message	IP Option Type <ipopt>: Bad Timestamp Pointer <tsptr>. Dropping
Explanation	The packet contains an invalid Timestamp Pointer. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt tsptr
Context Parameters	Rule Name Packet Buffer

2.25.14. bad_timestamp_pointer (ID: 01700019)

Default Severity	WARNING
Log Message	IP Option Type <ipopt>: Bad Timestamp Pointer <tsptr> with overflow <oflo>. Dropping
Explanation	The packet contains an invalid Timestamp Pointer, with Overflow. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt tsptr oflo
Context Parameters	Rule Name Packet Buffer

2.25.15. timestamp_disallowed (ID: 01700020)

Default Severity	WARNING
Log Message	Timestamp IP option disallowed. Dropping

Explanation	The packet contains a timestamp IP Option, which is disallowed. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.25.16. router_alert_bad_len (ID: 01700021)

Default Severity	WARNING
Log Message	IP Option Type <ipopt>: Bad length <optlen>. Dropping
Explanation	Packet contains a router alert IP Option, which has an invalid Length. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt optlen
Context Parameters	Rule Name Packet Buffer

2.25.17. router_alert_disallowed (ID: 01700022)

Default Severity	WARNING
Log Message	Router Alert IP Option disallowed. Dropping
Explanation	The packet contains a timestamp IP Option, which is disallowed. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.25.18. ipopt_present_disallowed (ID: 01700023)

Default Severity	WARNING
Log Message	IP Option <ipopt>(<optname>) is present. Dropping

Explanation	The packet contains an IP Option, which is disallowed. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipopt optname
Context Parameters	Rule Name Packet Buffer

2.26. IP_PROTO

These log messages refer to the **IP_PROTO (IP Protocol verification events)** category.

2.26.1. multicast_ethernet_ip_address_mismatch (ID: 07000011)

Default Severity	WARNING
Log Message	Received packet with a destination IP address <ip_multicast_addr> that does not match the Ethernet multicast address <eth_multicast_addr>
Explanation	A packet was received with an IP multicast Ethernet address as destination address. The IP address in the IP header does however not match it. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ip_multicast_addr eth_multicast_addr
Context Parameters	Rule Name Packet Buffer

2.26.2. invalid_ip4_header_length (ID: 07000012)

Default Severity	WARNING
Log Message	Invalid IP4 Header length - total length is <totlen> bytes. Dropping
Explanation	The packet contains an invalid IP4 Header Length. The total length is more than 64 Kb, which is not allowed. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	totlen
Context Parameters	Rule Name Packet Buffer

2.26.3. ttl_zero (ID: 07000013)

Default Severity	WARNING
Log Message	Received packet with zero TTL. Dropping
Explanation	A packet was received with a TTL (Time-To-Live) field set to zero,

	which is not allowed. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.26.4. ttl_low (ID: 07000014)

Default Severity	WARNING
Log Message	Received packet with too low TTL of <ttl>. Min TTL is <ttlmin>. Dropping
Explanation	The received packet has a TTL (Time-To-Live) field which is too low. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ttl ttlmin
Context Parameters	Rule Name Packet Buffer

2.26.5. ip_rsv_flag_set (ID: 07000015)

Default Severity	WARNING
Log Message	The IP Reserved Flag was set. Dropping
Explanation	The received packet has the IP Reserved Flag set. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.26.6. oversize_tcp (ID: 07000018)

Default Severity	WARNING
Log Message	Configured size limit for the TCP protocol exceeded. Dropping
Explanation	The configured size limit for the TCP protocol was exceeded.

	Dropping packet.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.26.7. invalid_tcp_header (ID: 07000019)

Default Severity	WARNING
Log Message	Invalid TCP header - IPDataLen=<ipdatalen>, TCPHdrLen=<tcphdrLen>. Dropping
Explanation	The TCP packet contains an invalid header. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipdatalen tcphdrLen
Context Parameters	Rule Name Packet Buffer

2.26.8. oversize_udp (ID: 07000021)

Default Severity	WARNING
Log Message	Configured size limit for the UDP protocol exceeded. Dropping
Explanation	The configured size limit for the UDP protocol was exceeded. Dropping packet.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.26.9. invalid_udp_header (ID: 07000022)

Default Severity	WARNING
-------------------------	---------

Log Message	Invalid UDP header - IPDataLen=<ipdatalen>, UDPTotLen=<udptotlen>. Dropping
Explanation	The UDP packet contains an invalid header. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipdatalen udptotlen
Context Parameters	Rule Name Packet Buffer

2.26.10. **oversize_icmp (ID: 07000023)**

Default Severity	WARNING
Log Message	Configured size limit for the ICMP protocol exceeded. Dropping
Explanation	The configured size limit for the ICMP protocol was exceeded. Dropping packet.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.26.11. **invalid_icmp_header (ID: 07000024)**

Default Severity	WARNING
Log Message	Invalid ICMP header - IPDataLen=<ipdatalen>, ICMPMinLen=<icmpminlen>. Dropping
Explanation	The ICMP packet contains an invalid header. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ipdatalen icmpminlen
Context Parameters	Rule Name Packet Buffer

2.26.12. `multicast_ethernet_ip_address_mismatch` (ID: 07000033)

Default Severity	WARNING
Log Message	Received packet with a destination IP address <ip_multicast_addr> that does not match the Ethernet multicast address <eth_multicast_addr>
Explanation	A packet was received with an IP multicast Ethernet address as destination address, but the IP address in the IP header does however not match it. This is a known exploit, though the gateway is currently configured to forward these packets.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	ip_multicast_addr eth_multicast_addr
Context Parameters	Rule Name Packet Buffer

2.26.13. `oversize_gre` (ID: 07000050)

Default Severity	WARNING
Log Message	Configured size limit for the GRE protocol exceeded. Dropping
Explanation	The configured size limit for the GRE protocol was exceeded. Dropping packet.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.26.14. `oversize_esp` (ID: 07000051)

Default Severity	WARNING
Log Message	Configured size limit for the ESP protocol exceeded. Dropping
Explanation	The configured size limit for the ESP protocol was exceeded. Dropping packet.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.

Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.26.15. **oversize_ah** (ID: 07000052)

Default Severity	WARNING
Log Message	Configured size limit for the AH protocol exceeded. Dropping
Explanation	The configured size limit for the AH protocol was exceeded. Dropping packet.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.26.16. **oversize_skip** (ID: 07000053)

Default Severity	WARNING
Log Message	Configured size limit for the SKIP protocol exceeded. Dropping
Explanation	The configured size limit for the SKIP protocol was exceeded. Dropping packet.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.26.17. **oversize_ospf** (ID: 07000054)

Default Severity	WARNING
Log Message	Configured size limit for the OSPF protocol exceeded. Dropping
Explanation	The configured size limit for the OSPF protocol was exceeded. Dropping packet.
Gateway Action	drop

Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.26.18. **oversize_ipip (ID: 07000055)**

Default Severity	WARNING
Log Message	Configured size limit for the IPIP protocol exceeded. Dropping
Explanation	The configured size limit for the IPIP protocol was exceeded. Dropping packet.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.26.19. **oversize_ipcomp (ID: 07000056)**

Default Severity	WARNING
Log Message	Configured size limit for the IPComp protocol exceeded. Dropping
Explanation	The configured size limit for the IPComp protocol was exceeded. Dropping packet.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.26.20. **oversize_l2tp (ID: 07000057)**

Default Severity	WARNING
Log Message	Configured size limit for the L2TP protocol exceeded. Dropping
Explanation	The configured size limit for the L2TP protocol was exceeded. Dropping packet.

Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.26.21. **oversize_ip (ID: 07000058)**

Default Severity	WARNING
Log Message	Configured size limit for IP protocol exceeded. Dropping
Explanation	The configured size limit for the IP protocol was exceeded. Dropping packet.
Gateway Action	drop
Recommended Action	This can be changed under the Advanced Settings section.
Revision	1
Parameters	proto
Context Parameters	Rule Name Packet Buffer

2.26.22. **fragmented_icmp (ID: 07000070)**

Default Severity	WARNING
Log Message	This ICMP type is not allowed to be fragmented. Dropping
Explanation	The ICMP type is not allowed to be fragmented. Only "Echo" and "EchoReply" are allowed to be fragmented. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.26.23. **invalid_icmp_data_too_small (ID: 07000071)**

Default Severity	WARNING
Log Message	Invalid ICMP data length. ICMPDataLen=<icmpdatalen> ICMPIPHdrMinLen=<icmpiphdrminlen>. Dropping
Explanation	The ICMP data is not large enough to contain an IPv4 Header.

	Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	icmpdatalen icmpiphdrminlen
Context Parameters	Rule Name Packet Buffer

2.26.24. invalid_icmp_data_ip_ver (ID: 07000072)

Default Severity	WARNING
Log Message	Invalid ICMP data. ICMPDataLen=<icmpdatalen> ICMPIPVer=<icmpipver>. Dropping
Explanation	An invalid IP version is specified in the ICMP data. Version 4 expected. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	icmpdatalen icmpipver
Context Parameters	Rule Name Packet Buffer

2.26.25. invalid_icmp_data_too_small (ID: 07000073)

Default Severity	WARNING
Log Message	Invalid ICMP data length. ICMPDataLen=<icmpdatalen> ICMIPHDrLen=<icmphdrLen>. Dropping
Explanation	The ICMP data length is invalid. It must be large enough for the actual header, and the header must specify that it is atleast 20 bytes long. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	icmpdatalen icmphdrLen
Context Parameters	Rule Name Packet Buffer

2.26.26. invalid_icmp_data_invalid_ip_length (ID: 07000074)

Default Severity	WARNING
Log Message	Invalid ICMP data length. ICMPDataLen=<icmpdatalen> ICMPIPDataLen=<icmpipdatalen> ICMPIPDataMinLen=<icmpipdataminlen>. Dropping
Explanation	The ICMP data length is invalid. The contained IP data must be atleast 8 bytes long. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	icmpdatalen icmpipdatalen icmpipdataminlen
Context Parameters	Rule Name Packet Buffer

2.26.27. invalid_icmp_data_invalid_paramprob (ID: 07000075)

Default Severity	WARNING
Log Message	Invalid ICMP ProbPtr. ICMPDataLen=<icmpdatalen> ICMPIPDataLen=<icmpipdatalen> ParamProbPtr=<paramprobptr>. Dropping
Explanation	Invalid ICMP Parameter Problem pointer. Parameter Problem pointer is not within the allowed range. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	icmpdatalen icmpipdatalen paramprobptr
Context Parameters	Rule Name Packet Buffer

2.27. L2TP

These log messages refer to the **L2TP (L2TP tunnel events)** category.

2.27.1. I2tpclient_resolve_successful (ID: 02800001)

Default Severity	NOTICE
Log Message	L2TP client <iface> resolved <remotegwname> to <remotegw>
Explanation	The L2TP client successfully resolved the DNS name of the remote gateway.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegwname remotegw

2.27.2. I2tpclient_resolve_failed (ID: 02800002)

Default Severity	WARNING
Log Message	L2TP client <iface> failed to resolve <remotegwname>
Explanation	The L2TP client failed to resolve the DNS name of the remote gateway.
Gateway Action	None
Recommended Action	Make sure you have configured the DNS name of the remote gateway and the DNS servers correctly.
Revision	1
Parameters	iface remotegwname

2.27.3. I2tpclient_init (ID: 02800003)

Default Severity	NOTICE
Log Message	L2TP client initialized, request sent to server on <remotegw>
Explanation	The L2TP client has been initialized and a request has been sent to the remote gateway.
Gateway Action	None
Recommended Action	None.
Revision	1

Parameters	iface remotegw
-------------------	-------------------

2.27.4. l2tp_connection_disallowed (ID: 02800004)

Default Severity	NOTICE
Log Message	L2TP connection disallowed according to rule <rule>! Tunnel ID: <tunnelid>, Session ID: <sessionid>
Explanation	The L2TP connection is disallowed according to the specified userauth rule.
Gateway Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	rule tunnelid sessionid

2.27.5. unknown_l2tp_auth_source (ID: 02800005)

Default Severity	WARNING
Log Message	Unknown L2TP authentication source for <rule>! Tunnel ID: <tunnelid>, Session ID: <sessionid>
Explanation	The authentication source for the specified userauth rule is unknown to the L2TP server.
Gateway Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	rule tunnelid sessionid

2.27.6. only_routes_set_up_by_server_iface_allowed (ID: 02800006)

Default Severity	WARNING
Log Message	L2TP server <iface> received a packet routed by a route not set up by the interface itself. Dropping packet
Explanation	The L2TP server received a packet that was routed to the interface by a route that was either manually configured or set up by another subsystem.
Gateway Action	drop

Recommended Action	Make sure no manually configured routes to the L2TP server interface exists in the configuration.
Revision	1
Parameters	iface

2.27.7. l2tp_session_closed (ID: 02800007)

Default Severity	NOTICE
Log Message	Closed L2TP session. Session ID: <sessionid>, Tunnel ID: <tunnelid>
Explanation	The L2TP session with the specified session ID has been closed. The session was set up using the specified tunnel.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface sessionid tunnelid

2.27.8. l2tp_tunnel_closed (ID: 02800008)

Default Severity	NOTICE
Log Message	Closed L2TP tunnel. Tunnel ID: <tunnelid>, Interface: <iface>.
Explanation	The L2TP tunnel with the specified tunnel ID has been closed.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface tunnelid

2.27.9. session_closed (ID: 02800009)

Default Severity	WARNING
Log Message	MPPE failed but is required, closing session <sessionid> to <remotegw> on <iface>
Explanation	MPPE is required by the configuration but the MPPE negotiation failed. Session will be closed.
Gateway Action	None
Recommended Action	Make sure the peer is capable of MPPE encryption, or disable the MPPE requirement.

Revision	1
Parameters	iface sessionid remotegw

2.27.10. l2tp_session_request (ID: 02800010)

Default Severity	NOTICE
Log Message	L2TP session request sent. Tunnel ID: <tunnelid>
Explanation	An L2TP session request has been sent over the specified L2TP tunnel.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid

2.27.11. l2tp_session_up (ID: 02800011)

Default Severity	NOTICE
Log Message	L2TP session up. Tunnel ID: <tunnelid>, Session ID: <sessionid>, Auth: <auth>, MPPE: <mppe>
Explanation	The L2TP session negotiation has completed successfully.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid sessionid auth mppe

2.27.12. l2tp_no_userauth_rule_found (ID: 02800014)

Default Severity	WARNING
Log Message	Did not find a matching userauth rule for this L2TP server! Tunnel ID: <tunnelid>, Session ID: <sessionid>
Explanation	The L2TP server was unsuccessful trying to find a matching userauth rule.
Gateway Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1

Parameters	tunnelid sessionid
-------------------	-----------------------

2.27.13. l2tp_session_request (ID: 02800015)

Default Severity	NOTICE
Log Message	L2TP session request received. Tunnel ID: <tunnelid>
Explanation	A new session request was received on the specified tunnel.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid

2.27.14. l2tp_session_up (ID: 02800016)

Default Severity	NOTICE
Log Message	L2TP session up. Tunnel ID: <tunnelid>, Session ID: <sessionid>, User: <user>, Auth: <auth>, MPPE: <mppe>, Assigned IP: <assigned_ip>
Explanation	The L2TP session negotiation has completed successfully.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid sessionid user auth mppe assigned_ip

2.27.15. failure_init_radius_accounting (ID: 02800017)

Default Severity	WARNING
Log Message	Failed to send Accounting Start to RADIUS Accounting Server. Accounting will be disabled
Explanation	Failed to send START message to RADIUS accounting server. RADIUS accounting will be disabled for this session.
Gateway Action	accounting_disabled
Recommended Action	Make sure the RADIUS accounting configuration is correct.
Revision	1

2.27.16. l2tpclient_tunnel_up (ID: 02800018)

Default Severity	NOTICE
Log Message	L2TP tunnel to <remotegw> is up. Tunnel ID: <tunnelid>
Explanation	L2TP tunnel negotiated successfully.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	tunnelid iface remotegw

2.27.17. malformed_packet (ID: 02800019)

Default Severity	WARNING
Log Message	Malformed packet received from <remotegw> on tunnel <iface>. Error code: <error_code>
Explanation	A malformed packet was received by the L2TP interface.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw error_code

2.27.18. waiting_for_ip_to_listen_on (ID: 02800050)

Default Severity	NOTICE
Log Message	L2TP server <iface> cannot start until it has an IP address to listen on
Explanation	The L2TP server cannot start until the L2TP interface has a proper IP address to listen on.
Gateway Action	None
Recommended Action	Make sure that the IP address is configured correctly on the L2TP server interface, or that the DHCP server can hand out a proper IP address to the interface.
Revision	1
Parameters	iface

2.28. LICUPDATE

These log messages refer to the **LICUPDATE (License update)** category.

2.28.1. license_update_failure (ID: 05500001)

Default Severity	ALERT
Log Message	License update failed, because of <reason>
Explanation	The unit tried to update the license, but failed. The reason for this is specified in the "reason" parameter.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason

2.28.2. license_downloaded (ID: 05500002)

Default Severity	NOTICE
Log Message	New license downloaded
Explanation	An updated license has been downloaded, which will now be used.
Gateway Action	using_new_license
Recommended Action	None.
Revision	1

2.28.3. license_already_up_to_date (ID: 05500003)

Default Severity	NOTICE
Log Message	License is up-to-date
Explanation	The current license is up-to-date, and does not need to be updated.
Gateway Action	None
Recommended Action	None.
Revision	1

2.29. NETCON

These log messages refer to the **NETCON (Netcon (remote mgmt) events)** category.

2.29.1. init_complete (ID: 02300001)

Default Severity	INFORMATIONAL
Log Message	NetCon initialization complete
Explanation	The NetCon initializing phase was successfully completed, and the unit can now process NetCon traffic.
Gateway Action	None
Recommended Action	None.
Revision	1

2.29.2. netcon_connect_reject_shutdown_running (ID: 02300002)

Default Severity	WARNING
Log Message	Rejecting NetCon connect attempt from <peer_ip>:<peer_port> - shutdown running
Explanation	A NetCon connection attempt was rejected, as the unit is shutting down.
Gateway Action	drop
Recommended Action	Try again when the unit is up and running.
Revision	1
Parameters	peer_ip peer_port

2.29.3. disallowed_netcon_ping (ID: 02300003)

Default Severity	WARNING
Log Message	Disallowed NetCon ping from <peer_ip>:<peer_port>
Explanation	The unit received a disallowed NetCon ping from peer.
Gateway Action	drop
Recommended Action	If this is a valid NetCon ping, make sure that the peer is configured to use NetCon.
Revision	1
Parameters	peer_ip peer_port

2.29.4. netcon_sessionmanager_error (ID: 02300101)

Default Severity	WARNING
Log Message	Missing context at Session Manager callback
Explanation	Incoming event from the Session Manager was for a nonexistent context.
Gateway Action	none
Recommended Action	Check current contexts in NetCon and in Session Manager.
Revision	1

2.29.5. cert_upload_aborted (ID: 02300200)

Default Severity	NOTICE
Log Message	Certificate upload from <peer_ip>:<peer_port> aborted by peer
Explanation	X.509 certificates were being uploaded, but the process was aborted by peer.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	peer_ip peer_port

2.29.6. cert_upload_failed (ID: 02300201)

Default Severity	ERROR
Log Message	Certificate upload from <peer_ip>:<peer_port> failed. Reason: <reason>
Explanation	Uploading of x.509 certificates to the unit failed. The "reason" parameter contains the reason for this.
Gateway Action	abort_transfer
Recommended Action	None.
Revision	1
Parameters	reason peer_ip peer_port

2.29.7. cert_upload_begin (ID: 02300202)

Default Severity	INFORMATIONAL
Log Message	Receiving certificates (<size> bytes) from <peer_ip>:<peer_port>
Explanation	Uploading of x.509 certificates to the unit is in progress.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	size peer_ip peer_port

2.29.8. upload_fail_disk_out_of_space (ID: 02300250)

Default Severity	ERROR
Log Message	Out of disk space receiving <upload_file> from <peer_ip>:<peer_port>
Explanation	The unit ran out of disk space when a file was being uploaded. The upload process was aborted.
Gateway Action	abort
Recommended Action	Verify that the disk media is intact, and remove old unused files.
Revision	1
Parameters	upload_file peer_ip peer_port

2.29.9. upload_fail_disk_cannot_remove (ID: 02300251)

Default Severity	ERROR
Log Message	Out of disk space receiving <upload_file> from <peer_ip>:<peer_port>, and failed to remove old file <old_file> because of <reason>.
Explanation	The unit ran out of disk space when a new version of an already existing file was being uploaded. The previous version of the file was not successfully removed. The upload process was aborted.
Gateway Action	abort
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	upload_file old_file reason peer_ip peer_port

2.29.10. disk_out_of_space (ID: 02300252)

Default Severity	NOTICE
Log Message	Out of disk space receiving <upload_file> from <peer_ip>:<peer_port>. Removed <old_file> to free up more space
Explanation	The unit ran out of disk space when a new version of an already existing file was being uploaded. The previous version of the file was successfully removed in order to free space, and the uploading process is resumed.
Gateway Action	removed_old_file
Recommended Action	None.
Revision	1
Parameters	upload_file old_file peer_ip peer_port

2.29.11. disk_write_error (ID: 02300300)

Default Severity	WARNING
Log Message	Write error while receiving <upload_file> from <peer_ip>:<peer_port>, because of <reason>
Explanation	There was an error when writing an uploaded file to the disk media. The "reason" parameter contains the reason for this.
Gateway Action	upload_fail
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	upload_file reason peer_ip peer_port

2.29.12. upload_complete (ID: 02300350)

Default Severity	NOTICE
Log Message	Received <upload_file> from <peer_ip>:<peer_port>, <filesize> bytes total
Explanation	The unit successfully received an uploaded file.
Gateway Action	None
Recommended Action	None.

Revision	1
Parameters	upload_file filesize peer_ip peer_port

2.29.13. concurrent_processing_limit_reached (ID: 02300400)

Default Severity	WARNING
Log Message	File event <event> from <peer_ip>:<peer_port> for <file> failed. Too many NetCon peers are processing files simultaneously
Explanation	The file event failed, as too many NetCon peers are processing files simultaneously.
Gateway Action	None
Recommended Action	Try again later, when less NetCon peers are processing files.
Revision	1
Parameters	event file peer_ip peer_port

2.29.14. netcon_init_fail_listen_socket_fail (ID: 02300500)

Default Severity	ERROR
Log Message	Internal Error: Could not create listening socket for NetCon
Explanation	The NetCon initializing phase failed, as the unit failed to set up a listening socket for NetCon traffic. A possible reason for this is that the unit ran out of memory.
Gateway Action	None
Recommended Action	Verify that the unit has enough RAM memory available.
Revision	1

2.29.15. netcon_init_fail_security_file_corrupt (ID: 02300501)

Default Severity	ERROR
Log Message	NetCon security file corrupt. NetCon disabled
Explanation	The NetCon security file was corrupt. NetCon has been disabled, and no NetCon traffic can be processed.

Gateway Action	netcon_disable
Recommended Action	Verify that the NetCon security file exists, and is valid. Also try to revert the unit to using the default NetCon keys.
Revision	1

2.29.16. **disallowed_netcon_connect (ID: 02300502)**

Default Severity	WARNING
Log Message	Disallowed NetCon connect attempt from <peer_ip>:<peer_port>. Dropping
Explanation	A NetCon connection attempt was disallowed, and the connection was dropped.
Gateway Action	drop
Recommended Action	If this is a valid NetCon connection attempt, make sure that the peer is configured to use NetCon.
Revision	1
Parameters	peer_ip peer_port

2.29.17. **netcon_connect (ID: 02300503)**

Default Severity	NOTICE
Log Message	New NetCon connection from <peer_ip>:<peer_port>
Explanation	A NetCon connection was successfully established.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	peer_ip peer_port

2.29.18. **netcon_disconnect (ID: 02300504)**

Default Severity	NOTICE
Log Message	Disconnecting NetCon peer <peer_ip>:<peer_port>
Explanation	A NetCon connection was disconnected.
Gateway Action	None
Recommended Action	None.
Revision	1

Parameters	peer_ip peer_port
-------------------	----------------------

2.29.19. disk_cannot_write (ID: 02300505)

Default Severity	ERROR
Log Message	Failed to save new keys <file>. Reverting to old keys
Explanation	The unit failed to save the new NetCon security keys, and reverted into using the old keys.
Gateway Action	reverting_to_old_keys
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	file

2.29.20. keychange_successful (ID: 02300506)

Default Severity	NOTICE
Log Message	New keys have been stored in <file>
Explanation	The new NetCon security keys was successfully stored, and is now used for NetCon traffic.
Gateway Action	using_new_keys
Recommended Action	None.
Revision	1
Parameters	file

2.29.21. keychange_fail (ID: 02300507)

Default Severity	ERROR
Log Message	Failed to establish bi-directional confirmation with peer of new keys. Reverting to old keys
Explanation	The unit failed to establish a connection back to peer, using the new NetCon security keys. It will try to revert to the previous NetCon security keys.
Gateway Action	reverting_to_old_keys
Recommended Action	Verify that the new NetCon keys are valid, and that both peers are using the same keys.
Revision	1

2.29.22. disk_cannot_read_old_keys (ID: 02300508)

Default Severity	ERROR
Log Message	Failed to read old keys from <file>
Explanation	The unit failed to read the old NetCon security keys from the security file.
Gateway Action	None
Recommended Action	Verify that the NetCon security file exists, and that it is valid. Try uploading a new Netcon secutiy file.
Revision	1
Parameters	file

2.29.23. download_fail (ID: 02300509)

Default Severity	ERROR
Log Message	File download requested by peer <peer_ip>:<peer_port> failed
Explanation	A peer requested to download a file from the unit, but the process failed.
Gateway Action	None
Recommended Action	Verify that the disk media is intact, and that the file exists.
Revision	1
Parameters	peer_ip peer_port

2.29.24. concurrent_netcon_processing (ID: 02300510)

Default Severity	ERROR
Log Message	File event <event> request from peer <peer_ip>:<peer_port> failed. The file <file> is currently being <current_event> by another NetCon peer.
Explanation	The file event, upload or download, failed, as another NetCon peer is currently carrying out the same event on the same file.
Gateway Action	None
Recommended Action	Try again later, when no other NetCon peer is uploading/downloading the file.
Revision	1
Parameters	event file current_event peer_ip

peer_port

2.29.25. disk_cannot_write (ID: 02300511)

Default Severity	ERROR
Log Message	Failed to open <file> for writing. Upload request from peer <peer_ip>:<peer_port> failed.
Explanation	The unit failed to open the file for write access, and as a result, the upload request failed.
Gateway Action	None
Recommended Action	Verify that the disk media is intact, and that this file is not write protected.
Revision	1
Parameters	file peer_ip peer_port

2.29.26. upload_begin (ID: 02300512)

Default Severity	NOTICE
Log Message	Receiving <file> from peer <peer_ip>:<peer_port>.
Explanation	The upload phase has begun, and the unit is currently receiving the file from peer, using chunked encoding.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	file peer_ip peer_port

2.29.27. upload_begin (ID: 02300513)

Default Severity	NOTICE
Log Message	Receiving <file> (<filesize> bytes) from peer <peer_ip>:<peer_port>.
Explanation	The upload phase has begun, and the unit is currently receiving the file, with the specified filesize, from peer.
Gateway Action	None
Recommended Action	None.
Revision	1

Parameters	file filesize peer_ip peer_port
-------------------	--

2.29.28. disk_cannot_read_download_fail (ID: 02300514)

Default Severity	ERROR
Log Message	Failed to open <file> for reading. Download request from peer <peer_ip>:<peer_port> failed.
Explanation	The unit failed to open the file for read access, and as a result, the download request failed.
Gateway Action	None
Recommended Action	Verify that the disk media is intact, and that this file is exists on the media.
Revision	1
Parameters	file peer_ip peer_port

2.29.29. download_begin (ID: 02300515)

Default Severity	NOTICE
Log Message	Sending <file> to peer <peer_ip>:<peer_port>.
Explanation	The download phase has begun, and the unit is currently sending the file to peer.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	file peer_ip peer_port

2.29.30. upload_abort (ID: 02300516)

Default Severity	NOTICE
Log Message	Upload from peer <peer_ip>:<peer_port> aborted by peer
Explanation	The upload process was aborted by peer. A partialy received file will be deleted.
Gateway Action	None
Recommended Action	None.

Revision	1
Parameters	peer_ip peer_port

2.29.31. upload_fail (ID: 02300517)

Default Severity	WARNING
Log Message	Upload of <file> peer <peer_ip>:<peer_port> failed because of <reason>
Explanation	The upload process failed. The "reason" parameter contains the reason for this.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	file reason peer_ip peer_port

2.29.32. download_complete (ID: 02300518)

Default Severity	NOTICE
Log Message	Sent <file> to peer <peer_ip>:<peer_port>, total <filesize> bytes
Explanation	The download phase was completed, and unit successfully sent the file to peer.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	file filesize peer_ip peer_port

2.30. OSPF

These log messages refer to the OSPF (OSPF events) category.

2.30.1. internal_error (ID: 02400001)

Default Severity	WARNING
Log Message	Internal Error. Iface <iface> got IEvent <ievent> in IState <istate>. Ignored
Explanation	Internal error in the OSPF interface state engine.
Gateway Action	ignore
Recommended Action	Contact support.
Revision	1
Parameters	iface ievent istate
Context Parameters	Rule Name

2.30.2. internal_error (ID: 02400002)

Default Severity	WARNING
Log Message	Internal Error. Iface <iface> got NEvent <nevent> in NState <nstate>. Ignored
Explanation	Internal error in the OSPF interface neighbor state engine.
Gateway Action	ignore
Recommended Action	Contact support.
Revision	1
Parameters	iface nevent nstate
Context Parameters	Rule Name

2.30.3. unable_to_map_ptp_neighbor (ID: 02400003)

Default Severity	WARNING
Log Message	Unable to map PTP neighbor <neighborid> to my ip <myifaceip> at HA failover
Explanation	Unable to map a configured PTP neighbor to the local IP at HA failover.
Gateway Action	None

Recommended Action	Check OSPF interface configuration.
Revision	1
Parameters	iface neighborid myifaceip
Context Parameters	Rule Name

2.30.4. bad_packet_len (ID: 02400004)

Default Severity	WARNING
Log Message	Received OSPF packet with bad length
Explanation	Received OSPF packet with a bad length.
Gateway Action	drop
Recommended Action	Check the configuration on the neighboring router.
Revision	1
Parameters	ospflen iplen type
Context Parameters	Rule Name Packet Buffer

2.30.5. bad_ospf_version (ID: 02400005)

Default Severity	WARNING
Log Message	Packet OSPF version is not 2
Explanation	Received OSPF packet with other version than 2.
Gateway Action	drop
Recommended Action	Make sure that all routers are using version 2.
Revision	1
Parameters	ver
Context Parameters	Rule Name Packet Buffer

2.30.6. sender_not_in_iface_range (ID: 02400006)

Default Severity	WARNING
Log Message	Sender source <srcip> not within interface range (<ifacorange>)
Explanation	Received OSPF data from a neighboring router not within the receive

	interface range.
Gateway Action	drop
Recommended Action	Make sure all locally attached OSPF routes are on the same network.
Revision	1
Parameters	srcip ifacorange
Context Parameters	Rule Name Packet Buffer

2.30.7. area_mismatch (ID: 02400007)

Default Severity	WARNING
Log Message	Bad area <area>
Explanation	Received OSPF data from a neighboring router not within the same area as the receive interface.
Gateway Action	drop
Recommended Action	Make sure all locally attached OSPF routers are in the same area as the attaching interfaces.
Revision	1
Parameters	area
Context Parameters	Rule Name Packet Buffer

2.30.8. hello_netmask_mismatch (ID: 02400008)

Default Severity	WARNING
Log Message	Hello netmask mismatch. Received was <recv_netmask>, mine is <my_netmask>. Dropping
Explanation	Received OSPF data from a neighboring router with different network netmask then the receive interface.
Gateway Action	drop
Recommended Action	Make sure all locally attached OSPF routers have the same netmask as the attaching interfaces.
Revision	1
Parameters	recv_netmask my_netmask
Context Parameters	Rule Name Packet Buffer

2.30.9. hello_interval_mismatch (ID: 02400009)

Default Severity	WARNING
Log Message	Hello interval mismatch. Received was <recv_interval>, mine is <my_interval>. Dropping
Explanation	Received OSPF data from a neighboring router with a mismatching hello interval.
Gateway Action	drop
Recommended Action	Make sure all locally attached OSPF routers share the same hello interval.
Revision	1
Parameters	recv_interval my_interval
Context Parameters	Rule Name Packet Buffer

2.30.10. hello_rtr_dead_mismatch (ID: 02400010)

Default Severity	WARNING
Log Message	Hello router dead interval mismatch. Received was <recv_rtrdead>, mine is <my_rtrdead>. Dropping
Explanation	Received OSPF data from a neighboring router with a mismatching router dead interval.
Gateway Action	drop
Recommended Action	Make sure all locally attached OSPF routers share the same router dead interval.
Revision	1
Parameters	recv_rtrdead my_rtrdead
Context Parameters	Rule Name Packet Buffer

2.30.11. hello_e_flag_mismatch (ID: 02400011)

Default Severity	WARNING
Log Message	Hello E-flag mismatch. Received was <recv_e_flag>, mine is <my_e_flag>. Dropping
Explanation	Received OSPF data from a neighboring router with mismatching E-flag (describes how AS-external-LSAs are flooded) configuration.
Gateway Action	drop

Recommended Action	Make sure all locally attached OSPF routers share the same E-flag configuration.
Revision	1
Parameters	recv_e_flag my_e_flag
Context Parameters	Rule Name Packet Buffer

2.30.12. hello_n_flag_mismatch (ID: 02400012)

Default Severity	WARNING
Log Message	Hello N-flag mismatch. Received was <recv_n_flag>, mine is <my_n_flag>. Dropping
Explanation	Received OSPF data from a neighboring router with mismatching N-flag (NSSA details) configuration.
Gateway Action	drop
Recommended Action	Make sure all locally attached OSPF routers share the same N-flag configuration.
Revision	1
Parameters	recv_n_flag my_n_flag
Context Parameters	Rule Name Packet Buffer

2.30.13. both_np_and_e_flag_set (ID: 02400013)

Default Severity	WARNING
Log Message	Hello N-flag and E-flag set. This is a illegal combination. Dropping
Explanation	Received OSPF data from a neighboring router which illegally have both the N and E-flag set.
Gateway Action	drop
Recommended Action	Check the configuration on the neighboring router.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.30.14. unknown_lsa_type (ID: 02400014)

Default Severity	WARNING
Log Message	Unknown LSA type <lsatype>. Dropping

Explanation	Received OSPF data from a neighbor which contained a unknown LSA.
Gateway Action	drop
Recommended Action	Check the configuration on the neighboring router.
Revision	1
Parameters	lsatype
Context Parameters	Rule Name Packet Buffer

2.30.15. auth_mismatch (ID: 02400050)

Default Severity	WARNING
Log Message	Authentication mismatch. Received was <recv_auth>, mine is <my_auth>
Explanation	Authentication mismatch with neighboring OSPF router.
Gateway Action	drop
Recommended Action	Verify that the neighboring OSPF router share the same authentication.
Revision	1
Parameters	recv_auth my_auth
Context Parameters	Rule Name

2.30.16. bad_auth_password (ID: 02400051)

Default Severity	WARNING
Log Message	Authentication mismatch. Bad password
Explanation	Authentication failed due to a bad password.
Gateway Action	drop
Recommended Action	Verify that the neighboring OSPF router share the same password.
Revision	1
Context Parameters	Rule Name

2.30.17. bad_auth_crypto_key_id (ID: 02400052)

Default Severity	WARNING
Log Message	Authentication mismatch. Bad crypto key id. Received was <recv_id>, mine is <my_id>

Explanation	Authentication failed due to a bad crypto key id.
Gateway Action	drop
Recommended Action	Verify that the neighboring OSPF router share the same crypto key id.
Revision	1
Parameters	recv_id my_id
Context Parameters	Rule Name

2.30.18. bad_auth_crypto_seq_number (ID: 02400053)

Default Severity	WARNING
Log Message	Authentication mismatch. Bad crypto sequence number. Received was <recv_seq>, expected atleast <my_seq>
Explanation	Authentication failed due to mismatching crypto sequence number.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	recv_seq my_seq
Context Parameters	Rule Name

2.30.19. bad_auth_crypto_digest (ID: 02400054)

Default Severity	WARNING
Log Message	Authentication mismatch. Bad crypto digest
Explanation	Authentication failed due to bad crypto digest.
Gateway Action	drop
Recommended Action	Verify that the neighboring OSPF router share the same crypto digest.
Revision	1
Context Parameters	Rule Name

2.30.20. checksum_mismatch (ID: 02400055)

Default Severity	WARNING
Log Message	Checksum mismatch. Received was <recv_chksum>, mine is <my_chksum>
Explanation	Received OSPF data from neighbor with mismatching checksum.

Gateway Action	drop
Recommended Action	Check network equipment for problems.
Revision	1
Parameters	recv_chksum my_chksum
Context Parameters	Rule Name

2.30.21. dd_mtu_exceeds_interface_mtu (ID: 02400100)

Default Severity	WARNING
Log Message	Neighbor <neighbor> MTU is too high. Received DD has MTU <dd_mtu>. Interface MTU is <iface_mtu>
Explanation	Received database description from neighbor with too high MTU.
Gateway Action	drop
Recommended Action	Lower the MTU on the neighboring OSPF router.
Revision	1
Parameters	neighbor dd_mtu iface_mtu
Context Parameters	Rule Name

2.30.22. m_ms_mismatch (ID: 02400101)

Default Severity	WARNING
Log Message	Neighbor <neighbor> M/MS mismatch. Restarting exchange
Explanation	Received indication that a neighbor got the M/MS (master/slave) role wrong.
Gateway Action	restart
Recommended Action	None.
Revision	1
Parameters	neighbor
Context Parameters	Rule Name

2.30.23. i_flag_misuse (ID: 02400102)

Default Severity	WARNING
Log Message	Neighbor <neighbor> misused the I-flag. Restarting exchange

Explanation	Neighbor misused the I-flag.
Gateway Action	restart
Recommended Action	None.
Revision	1
Parameters	neighbor
Context Parameters	Rule Name

2.30.24. opt_change (ID: 02400103)

Default Severity	WARNING
Log Message	Neighbor <neighbor> changed options during exchange. Restarting exchange
Explanation	Neighbor illegally changed options during the exchange phase.
Gateway Action	restart
Recommended Action	None.
Revision	1
Parameters	neighbor
Context Parameters	Rule Name

2.30.25. bad_seq_num (ID: 02400104)

Default Severity	WARNING
Log Message	Neighbor <neighbor> replied with a unexpected sequence number. Restarting exchange
Explanation	Received neighbor reply with a unexpected sequence number.
Gateway Action	restart
Recommended Action	None.
Revision	1
Parameters	neighbor
Context Parameters	Rule Name

2.30.26. non_dup_dd (ID: 02400105)

Default Severity	WARNING
Log Message	Neighbor <neighbor> sent a non dup DD from a higher state then exchange. Restarting exchange

Explanation	Received a non dup database descriptor from a neighbor in a higher state then exchange.
Gateway Action	restart
Recommended Action	None.
Revision	1
Parameters	neighbor
Context Parameters	Rule Name

2.30.27. as_ext_on_stub (ID: 02400106)

Default Severity	WARNING
Log Message	Neighbor <neighbor> implied AS-EXT on a stub area. Restarting exchange
Explanation	A neighbor illegally implied AS-EXT on a stub area.
Gateway Action	restart
Recommended Action	Check neighboring OSPF router configuration.
Revision	1
Parameters	neighbor
Context Parameters	Rule Name

2.30.28. unknown_lsa (ID: 02400107)

Default Severity	WARNING
Log Message	Neighbor <neighbor> implied unknown LSA (<lsa_type>). Restarting exchange
Explanation	A neighbor described an unknown LSA type.
Gateway Action	restart
Recommended Action	Check neighboring OSPF router configuration.
Revision	1
Parameters	neighbor lsa_type
Context Parameters	Rule Name

2.30.29. bad_lsa_sequence_number (ID: 02400108)

Default Severity	WARNING
Log Message	Got LSA with bad sequence number <seqnum>. Restarting exchange

Explanation	Received a LSA with a bad sequence number.
Gateway Action	restart
Recommended Action	None.
Revision	1
Parameters	seqnum
Context Parameters	Rule Name

2.30.30. bad_lsa_maxage (ID: 02400109)

Default Severity	WARNING
Log Message	Got LSA with bad maxage (<maxage> > <def_maxage>). Restarting exchange
Explanation	Received a LSA with a bad maxage value.
Gateway Action	restart
Recommended Action	Check orginating router configuration.
Revision	1
Parameters	maxage def_maxage
Context Parameters	Rule Name

2.30.31. lsa_checksum_mismatch (ID: 02400150)

Default Severity	WARNING
Log Message	LSA checksum mismatch. LSA is discarded
Explanation	Received LSA with mismatching checksum.
Gateway Action	discard
Recommended Action	Check network equipment for problems.
Revision	1
Context Parameters	Rule Name

2.30.32. unknown_lsa_type (ID: 02400151)

Default Severity	WARNING
Log Message	Unknown LSA type (<lsa_type>). LSA is discarded
Explanation	Received LSA of unknown type.
Gateway Action	discard

Recommended Action	Check originating router configuration.
Revision	1
Parameters	lsa_type
Context Parameters	Rule Name

2.30.33. bad_isa_sequencenumber (ID: 02400152)

Default Severity	WARNING
Log Message	Bad LSA sequence number (<seqnum>). LSA is discarded
Explanation	Received LSA with a bad sequence number.
Gateway Action	discard
Recommended Action	None.
Revision	1
Parameters	seqnum
Context Parameters	Rule Name

2.30.34. bad_isa_maxage (ID: 02400153)

Default Severity	WARNING
Log Message	Bad LSA maxage (<maxage>). LSA is discarded
Explanation	Received LSA with a bad max age.
Gateway Action	discard
Recommended Action	None.
Revision	1
Parameters	maxage
Context Parameters	Rule Name

2.30.35. received_as_ext_on_stub (ID: 02400154)

Default Severity	WARNING
Log Message	Received AS-EXT LSA on stub. LSA is discarded
Explanation	Received AS external LSA which is illegal on a stub area.
Gateway Action	discard
Recommended Action	None.
Revision	1

Context Parameters Rule Name

2.30.36. received_selforg_for_unknown_lsa_type (ID: 02400155)

Default Severity	WARNING
Log Message	Received selforginated LSA for unknown LSA <lsatype> type? Flushing
Explanation	Received selforginated LSA of unknown type.
Gateway Action	flush
Recommended Action	None.
Revision	1
Parameters	lsatype
Context Parameters	Rule Name

2.30.37. db_copy_more_recent_than_received (ID: 02400156)

Default Severity	WARNING
Log Message	Received LSA(LSA-<lsa> ID:<lsaid> AdvRtr:<lsartr>) is older than DB copy. Discarding received LSA
Explanation	Received LSA which is older than the copy in the database.
Gateway Action	discard
Recommended Action	None.
Revision	1
Parameters	lsa lsaid lsartr
Context Parameters	Rule Name

2.30.38. got_ack_mismatched_lsa (ID: 02400157)

Default Severity	WARNING
Log Message	Got ACK for mismatched LSA (LSA-<lsa> ID:<lsaid> AdvRtr:<lsartr>). ACK ignored
Explanation	Received acknowledge for mismatched LSA.
Gateway Action	None

Recommended Action	None.
Revision	1
Parameters	lsa lsaid lsartr
Context Parameters	Rule Name

2.30.39. upd_packet_lsa_size_mismatch (ID: 02400158)

Default Severity	WARNING
Log Message	UPD packet LSA size mismatch. Parsing aborted
Explanation	Received OSPF UPD packet with a mismatching LSA size.
Gateway Action	abort
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.30.40. req_packet_lsa_size_mismatch (ID: 02400159)

Default Severity	WARNING
Log Message	REQ packet LSA size mismatch. Parsing aborted
Explanation	Received OSPF REQ packet with a mismatching LSA size.
Gateway Action	abort
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.30.41. ack_packet_lsa_size_mismatch (ID: 02400160)

Default Severity	WARNING
Log Message	ACK packet LSA size mismatch. Parsing aborted
Explanation	Received OSPF ACK packet with a mismatching LSA size.
Gateway Action	abort
Recommended Action	None.
Revision	1

Context Parameters	Rule Name Packet Buffer
--------------------	----------------------------

2.30.42. failed_to_create_replacement_Isa (ID: 02400161)

Default Severity	CRITICAL
Log Message	Failed to prepare replacement LSA (LSA- <lsa> ID:<lsaid> AdvRtr:<lsartr>)
Explanation	Failed to create LSA.
Gateway Action	alert
Recommended Action	Check memory consumption.
Revision	1
Parameters	lsa lsaid lsartr
Context Parameters	Rule Name

2.30.43. unable_to_send_ack (ID: 02400162)

Default Severity	CRITICAL
Log Message	Unable to send ACK
Explanation	Unable to send acknowledgement.
Gateway Action	alert
Recommended Action	Check memory consumption.
Revision	1
Context Parameters	Rule Name

2.30.44. unknown_neighbor (ID: 02400200)

Default Severity	WARNING
Log Message	Unknown neighbor(IP:<neighbor> ID:<neighborid>) seen on <iface>. Ignoring
Explanation	Unknown neighbor seen on PTP based interface.
Gateway Action	None
Recommended Action	Check for incorrectly configured neighbors.
Revision	1
Parameters	neighbor neighborid

	iface
Context Parameters	Rule Name

2.30.45. too_many_neighbors (ID: 02400201)

Default Severity	WARNING
Log Message	Too many neighbors on <iface>. Unable to maintain 2-way with all of them(hello packet)
Explanation	There are too many OSPF routers on a directly connected network.
Gateway Action	None
Recommended Action	Reduce the number of OSPF routers on the network.
Revision	1
Parameters	iface
Context Parameters	Rule Name

2.30.46. neighbor_died (ID: 02400202)

Default Severity	WARNING
Log Message	Neighbor <neighbor> on <neighboriface> died
Explanation	Lost connectivity with neighbor router.
Gateway Action	None
Recommended Action	Check neighbor status and connectivity.
Revision	1
Parameters	neighbor neighboriface
Context Parameters	Rule Name

2.30.47. unable_to_find_transport_area (ID: 02400300)

Default Severity	WARNING
Log Message	Unable to find transport area <area> for VLINK <vlink> when building router LSA. Iface skipped
Explanation	Unable to find transport area for a vlink.
Gateway Action	skip_iface
Recommended Action	Check OSPF area configuration.
Revision	1

Parameters	area vlink
Context Parameters	Rule Name

2.30.48. internal_error_unable_to_map_identifier (ID: 02400301)

Default Severity	WARNING
Log Message	Internal error: Unable to map a identifier for LSA Type:<lsatype> ID:<lsaid> AdvRouter:<lsaadvtr>
Explanation	Unable to map an identifier for a LSA.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	lsatype lsaid lsaadvtr
Context Parameters	Rule Name

2.30.49. lsa_size_too_big (ID: 02400302)

Default Severity	WARNING
Log Message	Requested LSA size(<lsasize>) too big. Unable to create LSA
Explanation	Unable to create LSA since the size is too big.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	lsasize
Context Parameters	Rule Name

2.30.50. memory_usage_exceeded_70_percent_of_max_allowed (ID: 02400303)

Default Severity	WARNING
Log Message	Memory usage for OSPF process <ospfproc> have now exceeded 70 percent of the maximum allowed
Explanation	The memory usage for a OSPF process have exceeded 70 percent of the maximum allowed.

Gateway Action	None
Recommended Action	Check memory consumption.
Revision	1
Parameters	ospfproc
Context Parameters	Rule Name

2.30.51. memory_usage_exceeded_90_percent_of_max_allowed (ID: 02400304)

Default Severity	WARNING
Log Message	Memory usage for OSPF process <ospfproc> have now exceeded 90 percent of the maximum allowed
Explanation	The memory usage for a OSPF process have exceeded 70 percent of the maximum allowed.
Gateway Action	None
Recommended Action	Check memory consumption.
Revision	1
Parameters	ospfproc
Context Parameters	Rule Name

2.30.52. as_disabled_due_to_mem_alloc_fail (ID: 02400305)

Default Severity	CRITICAL
Log Message	AS disabled due to memory allocation failure
Explanation	An OSPF AS have been disabled due to memory allocation failure.
Gateway Action	alert
Recommended Action	Check memory consumption.
Revision	1
Context Parameters	Rule Name

2.30.53. internal_lsa_chksum_error (ID: 02400306)

Default Severity	CRITICAL
Log Message	LSA internal checksum error
Explanation	Internal LSA checksum error.
Gateway Action	alert

Recommended Action	Check hardware for defects.
Revision	1
Context Parameters	Rule Name

2.30.54. unable_to_find_iface_to_stub_net (ID: 02400400)

Default Severity	WARNING
Log Message	Internal error: Unable to find my interface attached to stub network <stub>
Explanation	Unable to find local interface attached to stub network.
Gateway Action	None
Recommended Action	Contact support with a scenario description.
Revision	1
Parameters	stub
Context Parameters	Rule Name

2.30.55. internal_error_unable_to_find_lnk_connecting_to_lsa (ID: 02400401)

Default Severity	WARNING
Log Message	Internal error: Unable to find my link connecting to described LSA (NetVtxId: <netvtxid>)
Explanation	Unable to find local link to described LSA.
Gateway Action	None
Recommended Action	Contact support with a scenario description.
Revision	1
Parameters	netvtxid
Context Parameters	Rule Name

2.30.56. internal_error_unable_to_find_iface_connecting_to_lsa (ID: 02400402)

Default Severity	WARNING
Log Message	Internal error: Unable to find my interface connecting to described LSA (NetVtxId: <netvtxid>)
Explanation	Unable to find local interface connecting to described LSA.
Gateway Action	None

Recommended Action	Contact support with a scenario description.
Revision	1
Parameters	netvtxid
Context Parameters	Rule Name

2.30.57. internal_error_unable_to_find_lnk_connecting_to_lsa (ID: 02400403)

Default Severity	WARNING
Log Message	Internal error: Unable to find my link connecting to described LSA (RtrVtxId: <rtrvtxid>)
Explanation	Unable to find local link connecting to described LSA.
Gateway Action	None
Recommended Action	Contact support with a scenario description.
Revision	1
Parameters	rtrvtxid
Context Parameters	Rule Name

2.30.58. internal_error_unable_to_find_iface_connecting_to_lsa (ID: 02400404)

Default Severity	WARNING
Log Message	Internal error: Unable to find my interface connecting to described LSA (RtrVtxId: <rtrvtxid>)
Explanation	Unable to find local interface connecting to described LSA.
Gateway Action	None
Recommended Action	Contact support with a scenario description.
Revision	1
Parameters	rtrvtxid
Context Parameters	Rule Name

2.30.59. internal_error_unable_neighbor_iface_attached_back_to_me (ID: 02400405)

Default Severity	WARNING
Log Message	Internal error: Unable to find neighbor (RtrVtxId: <rtrvtxid>) interface attached back to me

Explanation	Unable to find neighbor interface attached back.
Gateway Action	None
Recommended Action	Contact support with a scenario description.
Revision	1
Parameters	rtrvtxid
Context Parameters	Rule Name

2.30.60. bad_iface_type_mapping_rtr_to_rtr_link (ID: 02400406)

Default Severity	WARNING
Log Message	Internal error: Bad interface type (<ifacetype>) when mapping rtr-to-rtr (RtrVtxId:<rtrvtxid>)
Explanation	Bad interface type found when doing router-to-router mapping.
Gateway Action	None
Recommended Action	Check OSPF interface configuration.
Revision	1
Parameters	ifacetype rtrvtxid
Context Parameters	Rule Name

2.30.61. internal_error_unable_to_find_lnk_connecting_to_lsa (ID: 02400407)

Default Severity	WARNING
Log Message	Internal error: Unable to find my link connecting to described LSA (NetVtxId:<netvtxid>)
Explanation	Unable to find local link connected to described LSA.
Gateway Action	None
Recommended Action	Contact support with a scenario description.
Revision	1
Parameters	netvtxid
Context Parameters	Rule Name

2.30.62. memory_allocation_failure (ID: 02400500)

Default Severity	CRITICAL
-------------------------	----------

Log Message	Internal Error: Memory allocation failure! OSPF process now considered inconsistent
Explanation	Memory allocation failure.
Gateway Action	alert
Recommended Action	Check memory consumption.
Revision	1
Context Parameters	Rule Name

2.30.63. unable_to_send (ID: 02400501)

Default Severity	CRITICAL
Log Message	Internal Error: Unable to send (No sendbuffer?)
Explanation	Unable to get buffer for sending.
Gateway Action	alert
Recommended Action	Check buffer consumption.
Revision	1
Context Parameters	Rule Name

2.30.64. failed_to_add_route (ID: 02400502)

Default Severity	CRITICAL
Log Message	Failed to add route <route>! OSPF process should now be considered inconsistent
Explanation	Unable to add route.
Gateway Action	alert
Recommended Action	Check memory consumption.
Revision	1
Parameters	route
Context Parameters	Rule Name

2.31. PPP

These log messages refer to the **PPP (PPP tunnel events)** category.

2.31.1. ip_pool_empty (ID: 02500001)

Default Severity	WARNING
Log Message	IPCP can not assign IP address to peer because the IP address pool is empty
Explanation	IPCP can not assign an IP address to the peer because there are no free IP addresses in IP address pool.
Gateway Action	failed_ipcp_address_assignment
Recommended Action	Increase the number of IP addresses in the IP address pool to allow all connecting clients to be assigned a unique IP address.
Revision	1
Parameters	tunnel_type

2.31.2. ip_address_required_but_not_received (ID: 02500002)

Default Severity	WARNING
Log Message	IP address required but not received. PPP terminated
Explanation	Peer refuses to give out an IP address. Since an IP address lease is required, PPP is terminated.
Gateway Action	ppp_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.31.3. primary_dns_address_required_but_not_received (ID: 02500003)

Default Severity	WARNING
Log Message	Primary DNS address required but not received. PPP terminated
Explanation	Peer refuses to give out a primary DNS address. Since reception of a primary DNS address is required, PPP is terminated.
Gateway Action	ppp_terminated
Recommended Action	None.

Revision	1
Parameters	tunnel_type

2.31.4. **secondary_dns_address_required_but_not_received** (ID: 02500004)

Default Severity	WARNING
Log Message	Secondary DNS address required but not received. PPP terminated
Explanation	Peer refuses to give out a secondary DNS address. Since reception of a secondary DNS address is required, PPP is terminated.
Gateway Action	ppp_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.31.5. **primary_nbns_address_required_but_not_received** (ID: 02500005)

Default Severity	WARNING
Log Message	Primary NBNS address required but not received. PPP terminated
Explanation	Peer refuses to give out a primary NBNS address. Since reception of a primary NBNS address is required, PPP is terminated.
Gateway Action	ppp_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.31.6. **secondary_nbns_address_required_but_not_received** (ID: 02500006)

Default Severity	WARNING
Log Message	Secondary NBNS address required but not received. PPP terminated
Explanation	Peer refuses to give out a secondary NBNS address. Since reception of a secondary NBNS address is required, PPP is terminated.
Gateway Action	ppp_terminated
Recommended Action	None.
Revision	1

Parameters tunnel_type

2.31.7. failed_to_agree_on_authentication_protocol (ID: 02500050)

Default Severity	ERROR
Log Message	Failed to agree on authentication protocol. PPP terminated
Explanation	Failed to agree on PPP authentication protocol. PPP is terminated.
Gateway Action	ppp_terminated
Recommended Action	Review the allowed authentication protocols configured. The client and server must be configured to have at least one authentication protocol in common.
Revision	1
Parameters	tunnel_type

2.31.8. peer_refuses_to_use_authentication (ID: 02500051)

Default Severity	ERROR
Log Message	Peer refuses to use authentication. PPP terminated
Explanation	Peer refuses to use any authentication at all. PPP is terminated since we demand authentication.
Gateway Action	ppp_terminated
Recommended Action	Review the allowed authentication types configured. The client and server must be configured to have at least one authentication type in common.
Revision	1
Parameters	tunnel_type

2.31.9. lcp_negotiation_stalled (ID: 02500052)

Default Severity	ERROR
Log Message	LCP negotiation stalled. PPP terminated
Explanation	PPP LCP negotiation stalled. Terminating PPP since the peer persistently demands the use of an LCP option that is unsupported.
Gateway Action	ppp_terminated
Recommended Action	Try to reconfigure the peer so it does not demand the use of this LCP option.
Revision	1

Parameters	tunnel_type unsupported_lcp_option
-------------------	---------------------------------------

2.31.10. ppp_tunnel_limit_exceeded (ID: 02500100)

Default Severity	ALERT
Log Message	PPP Tunnel license limit exceeded. PPP terminated
Explanation	PPP is terminated because the license restrictions do not allow any more PPP tunnels. No new PPP tunnels can be established until an existing one is closed.
Gateway Action	ppp_terminated
Recommended Action	Upgrade your license to allow more simultaneous PPP tunnels.
Revision	1
Parameters	tunnel_type limit

2.31.11. authentication_failed (ID: 02500101)

Default Severity	WARNING
Log Message	Authentication failed. PPP terminated
Explanation	Authentication failed. PPP terminated.
Gateway Action	ppp_terminated
Recommended Action	Make sure that the right username and password is used.
Revision	1
Parameters	tunnel_type user

2.31.12. response_value_too_long (ID: 02500150)

Default Severity	WARNING
Log Message	PPP CHAP response value was truncated because it was too long
Explanation	PPP CHAP response value was truncated because it was too long.
Gateway Action	chap_response_value_truncated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.31.13. username_too_long (ID: 02500151)

Default Severity	WARNING
Log Message	PPP CHAP username was truncated because it was too long
Explanation	PPP CHAP username was truncated because it was too long.
Gateway Action	chap_username_truncated
Recommended Action	Reconfigure the endpoints to use a shorter username.
Revision	1
Parameters	tunnel_type

2.31.14. username_too_long (ID: 02500201)

Default Severity	WARNING
Log Message	PPP MSCHAPv1 username was truncated because it was too long
Explanation	PPP MSCHAPv1 username was truncated because it was too long.
Gateway Action	mschapv1_username_truncated
Recommended Action	Reconfigure the endpoints to use a shorter username.
Revision	1
Parameters	tunnel_type

2.31.15. username_too_long (ID: 02500301)

Default Severity	WARNING
Log Message	PPP MSCHAPv2 username was truncated because it was too long
Explanation	PPP MSCHAPv2 username was truncated because it was too long.
Gateway Action	mschapv2_username_truncated
Recommended Action	Reconfigure the endpoints to use a shorter username.
Revision	1
Parameters	tunnel_type

2.31.16. username_too_long (ID: 02500350)

Default Severity	WARNING
Log Message	PPP PAP username was truncated because it was too long
Explanation	PPP PAP username was truncated because it was too long.

Gateway Action	pap_username_truncated
Recommended Action	Reconfigure the endpoints to use a shorter username.
Revision	1
Parameters	tunnel_type

2.31.17. password_too_long (ID: 02500351)

Default Severity	WARNING
Log Message	PPP PAP password was truncated because it was too long
Explanation	PPP PAP password was truncated because it was too long.
Gateway Action	pap_password_truncated
Recommended Action	Reconfigure the endpoints to use a shorter password.
Revision	1
Parameters	tunnel_type

2.31.18. unsupported_auth_server (ID: 02500500)

Default Severity	ERROR
Log Message	Unsupported authentication server. PPP Authentication terminated
Explanation	Unsupported authentication server. PPP Authentication terminated.
Gateway Action	authentication_terminated
Recommended Action	Review the authentication server configuration.
Revision	1
Parameters	tunnel_type

2.31.19. radius_error (ID: 02500501)

Default Severity	ERROR
Log Message	Radius server authentication error. PPP Authentication terminated
Explanation	There was an error while authenticating using a radius server. PPP Authentication terminated.
Gateway Action	authentication_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.31.20. authdb_error (ID: 02500502)

Default Severity	ERROR
Log Message	Local database authentication error. PPP Authentication terminated
Explanation	There was an error while authenticating using a local user database. PPP Authentication terminated.
Gateway Action	authentication_terminated
Recommended Action	None.
Revision	1
Parameters	tunnel_type

2.31.21. MPPE_decrypt_fail (ID: 02500600)

Default Severity	ERROR
Log Message	MPPE decryption resulted in the unsupported protocol <protocol>. Terminating PPP
Explanation	MPPE decryption resulted in an unsupported protocol. IP is the only protocol supported. This either means that the decryption failed or that the peer actually sent data using an unsupported protocol. PPP is terminated.
Gateway Action	ppp_terminated
Recommended Action	Reconnect the tunnel. If the peer keeps sending the same unsupported protocol, try to reconfigure the peer to only send IP packets through the tunnel.
Revision	1
Parameters	protocol

2.32. PPPOE

These log messages refer to the **PPPOE (PPPoE tunnel events)** category.

2.32.1. pppoe_tunnel_up (ID: 02600001)

Default Severity	NOTICE
Log Message	PPPoE tunnel on <iface> established to <pppoeserver>. Auth: <auth>, IfaceIP: <ifaceip>, Downtime: <downtime>
Explanation	The PPPoE tunnel for the interface have been established. .
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface pppoeserver auth ifaceip downtime

2.32.2. pppoe_tunnel_closed (ID: 02600002)

Default Severity	NOTICE
Log Message	PPPoE tunnel on <iface> to <pppoeserver> closed. Uptime: <uptime>
Explanation	The PPPoE tunnel for the interface have been closed. .
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface pppoeserver uptime

2.33. PPTP

These log messages refer to the **PPTP (PPTP tunnel events)** category.

2.33.1. pptpclient_resolve_successful (ID: 02700001)

Default Severity	NOTICE
Log Message	PPTP client <iface> resolved <remotegwname> to <remotegw>
Explanation	The PPTP client successfully resolved the DNS name of remote gateway.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegwname remotegw

2.33.2. pptpclient_resolve_failed (ID: 02700002)

Default Severity	WARNING
Log Message	PPTP client <iface> failed to resolve <remotegwname>
Explanation	The PPTP client failed to resolve the DNS name of the remote gateway.
Gateway Action	None
Recommended Action	Make sure you have configured the DNS name of the remote gateway and the DNS servers correctly.
Revision	1
Parameters	iface remotegwname

2.33.3. pptp_connection_disallowed (ID: 02700003)

Default Severity	WARNING
Log Message	PPTP connection from <remotegw> disallowed according to rule <rule>! Call ID: <callid>
Explanation	The PPTP connection is disallowed by the new configuration according to the specified userauth rule. Closing down the PPTP connection.
Gateway Action	pptp_connection_closed
Recommended Action	Make sure the userauth rules are configured correctly.

Revision	1
Parameters	rule remotegw callid

2.33.4. unknown_pptp_auth_source (ID: 02700004)

Default Severity	WARNING
Log Message	Unknown PPTP authentication source for <rule>! Remote gateway: <remotegw>, Call ID: <callid>
Explanation	The authentication source for the specified userauth rule found in the new configuration is unknown to the PPTP server. Closing down the PPTP connection.
Gateway Action	pptp_connection_closed
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	rule remotegw callid

2.33.5. user_disconnected (ID: 02700005)

Default Severity	WARNING
Log Message	User <user> is forcibly disconnected. Call ID: <callid> Remote gateway: <remotegw>
Explanation	The connected client is forcibly disconnected by the userauth system.
Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	user callid remotegw

2.33.6. only_routes_set_up_by_server_iface_allowed (ID: 02700006)

Default Severity	WARNING
Log Message	PPTP server <iface> received a packet routed by a route not set up by the interface itself. Dropping packet.
Explanation	The PPTP server interface received a packet that was routed to the interface by a route that was either manually configured or set up by

	another subsystem. Traffic can only be sent out on the PPTP server using the dynamic routes set up by the interface itself.
Gateway Action	drop
Recommended Action	Make sure there are no manually configured routes pointing to the PPTP server interface in the configuration.
Revision	1
Parameters	iface

2.33.7. mppe_required (ID: 02700007)

Default Severity	WARNING
Log Message	MPPE failed but is required, closing session <callid> to <remotegw> on <iface>.
Explanation	MPPE is required by the configuration but the MPPE negotiation failed. Session will be closed.
Gateway Action	close_session
Recommended Action	Make sure the peer is capable of MPPE encryption, or disable the MPPE requirement.
Revision	1
Parameters	iface remotegw callid

2.33.8. pptp_session_closed (ID: 02700008)

Default Severity	NOTICE
Log Message	PPTP session <callid> to <remotegw> on <iface> closed.
Explanation	A PPTP session has been closed. The specified interface, remote gateway and call ID identify the specific session.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw callid

2.33.9. pptp_session_request (ID: 02700009)

Default Severity	NOTICE
Log Message	PPTP session request sent on control connection to <remotegw>

Explanation	An PPTP session request has been sent on the control connection to the specified remote gateway.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	remotegw

2.33.10. unsupported_message (ID: 02700010)

Default Severity	WARNING
Log Message	Unsupported message type <type> received on session <callid> from <remotegw>. Ignoring message.
Explanation	A message with unsupported type received. Ignoring it. The specified interface, remote gateway and call ID identify the specific session.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	iface type callid remotegw

2.33.11. failure_init_radius_accounting (ID: 02700011)

Default Severity	WARNING
Log Message	Failed to send Accounting Start to RADIUS Accounting Server. Accounting will be disabled. Interface: <iface>, Remote gateway: <remotegw>, Call ID: <callid>
Explanation	Failed to send START message to RADIUS accounting server. RADIUS accounting will be disabled for this session. The specified interface, remote gateway and call ID identify the specific session.
Gateway Action	accounting_disabled
Recommended Action	Make sure the RADIUS accounting configuration is correct.
Revision	1
Parameters	callid remotegw iface

2.33.12. pptp_session_up (ID: 02700012)

Default Severity	WARNING
-------------------------	---------

Log Message	PPP negotiation completed for session <callid> to <remotegw> on <iface>. User: <user>, Auth: <auth>, MPPE: <mppe>, Assigned IP: <assigned_ip>
Explanation	The PPP negotiation has completed successfully for this session. The specified interface, remote gateway and call ID identify the specific session.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	callid iface remotegw user auth mppe assigned_ip

2.33.13. pptp_session_up (ID: 02700013)

Default Severity	WARNING
Log Message	PPP negotiation completed for session <callid> on <iface> connected to <remotegw>. Auth: <auth>, MPPE: <mppe>
Explanation	The PPP negotiation has completed successfully for this session. The specified interface, remote gateway and call ID identify the specific session.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	callid iface remotegw auth mppe

2.33.14. tunnel_idle_timeout (ID: 02700014)

Default Severity	WARNING
Log Message	PPTP tunnel to <remotegw> on <iface> has been idle for too long. Closing it.
Explanation	A PPTP tunnel has been idle for too long. Tunnel will be closed.
Gateway Action	close_tunnel
Recommended Action	None.
Revision	1

Parameters	iface remotegw
-------------------	-------------------

2.33.15. session_idle_timeout (ID: 02700015)

Default Severity	WARNING
Log Message	PPTP session <callid> to <remotegw> on <iface> has been idle for too long. Closing it.
Explanation	A PPTP session has been idle for too long. Session will be closed.
Gateway Action	close_session
Recommended Action	None.
Revision	1
Parameters	iface remotegw callid

2.33.16. pptpclient_start (ID: 02700017)

Default Severity	NOTICE
Log Message	PPTP client <iface> started, connecting to server on <remotegw>
Explanation	A PPTP client has initiated the connection to its remote gateway.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.33.17. pptpclient_connected (ID: 02700018)

Default Severity	NOTICE
Log Message	PPTP client <iface> connected to <remotegw>, requesting control connection
Explanation	A PPTP client has established a connection to its remote gateway and is sending a control connection request message.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.33.18. pptp_tunnel_up (ID: 02700019)

Default Severity	NOTICE
Log Message	PPTP tunnel up, client <remotegw> connected to <iface>
Explanation	A remote PPTP client has established a connection to this PPTP server.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.33.19. ctrlconn_refused (ID: 02700020)

Default Severity	WARNING
Log Message	The remote PPTP server on <remotegw> refused to establish PPTP control connection. Reason: <reason>
Explanation	A remote PPTP server refused to establish PPTP control connection.
Gateway Action	None
Recommended Action	Read the reason specified by the PPTP server. This might give a clue why the PPTP server refused the PPTP control connection.
Revision	1
Parameters	reason iface remotegw

2.33.20. pptp_tunnel_up (ID: 02700021)

Default Severity	NOTICE
Log Message	PPTP tunnel on <iface> is up. Connected to server on <remotegw>.
Explanation	This PPTP client has established a control connection to the remote PPTP server.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.33.21. pptp_tunnel_closed (ID: 02700022)

Default Severity	NOTICE
Log Message	PPTP tunnel to <remotegw> on <iface> closed.
Explanation	The PPTP tunnel to has been closed.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw

2.33.22. pptp_connection_disallowed (ID: 02700024)

Default Severity	WARNING
Log Message	PPTP connection from <remotegw> disallowed according to rule <rule>. Interface: <iface>.
Explanation	The PPTP connection is disallowed according to the specified userauth rule.
Gateway Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	rule iface remotegw

2.33.23. unknown_pptp_auth_source (ID: 02700025)

Default Severity	WARNING
Log Message	Unknown PPTP authentication source for <rule>!. Interface: <iface>, Remote gateway: <remotegw>.
Explanation	The authentication source for the specified userauth rule is unknown to the PPTP server.
Gateway Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	rule iface remotegw

2.33.24. pptp_no_userauth_rule_found (ID: 02700026)

Default Severity	WARNING
Log Message	Did not find a matching userauth rule for the incoming PPTP connection. Interface: <iface>, Remote gateway: <remotegw>.
Explanation	The PPTP server was unsuccessful trying to find a userauth rule matching the incoming PPTP connection.
Gateway Action	None
Recommended Action	Make sure the userauth rules are configured correctly.
Revision	1
Parameters	iface remotegw

2.33.25. malformed_packet (ID: 02700027)

Default Severity	WARNING
Log Message	Malformed packet received from <remotegw> on <iface>. Error code: <error_code>
Explanation	A malformed packet was received by the PPTP interface.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	iface remotegw error_code

2.33.26. waiting_for_ip_to_listen_on (ID: 02700050)

Default Severity	WARNING
Log Message	PPTP server <iface> cannot start until it has an IP address to listen on.
Explanation	The PPTP server cannot start until it has a proper IP address to listen on.
Gateway Action	None
Recommended Action	Make sure that the IP address is configured correctly on the PPTP server interface. If the PPTP server is supposed to listen on an IP assigned by a DHCP server, make sure that the DHCP server is working properly.
Revision	1
Parameters	iface

2.34. REASSEMBLY

These log messages refer to the **REASSEMBLY (Events concerning data reassembly)** category.

2.34.1. ack_of_not_transmitted_data (ID: 04800002)

Default Severity	INFORMATIONAL
Log Message	TCP segment acknowledges data not yet transmitted
Explanation	A TCP segment that acknowledges data not yet transmitted was received. The segment will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Connection

2.34.2. invalid_tcp_checksum (ID: 04800003)

Default Severity	NOTICE
Log Message	TCP segment with invalid checksum
Explanation	A TCP segment with an invalid checksum was received. The segment will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Connection

2.34.3. mismatching_data_in_overlapping_tcp_segment (ID: 04800004)

Default Severity	ERROR
Log Message	Overlapping TCP segment containing different data
Explanation	A TCP segment that partly overlaps segments that has been received earlier was received. The data in the overlapping part is however different from the data in the segments received earlier. The segment's data will be replaced so that it is consistent with the earlier received segments.
Gateway Action	correct the data
Recommended Action	Research the source of this erroneous traffic.
Revision	1

Context Parameters	Connection
--------------------	------------

2.34.4. memory_allocation_failure (ID: 04800005)

Default Severity	ERROR
Log Message	Can't allocate memory to keep track of a packet
Explanation	The gateway is unable to allocate memory to keep track of packet that was received. The packet will be dropped.
Gateway Action	drop
Recommended Action	Review configuration to reduce memory consumption.
Revision	1

2.34.5. drop_due_to_buffer_starvation (ID: 04800007)

Default Severity	ERROR
Log Message	Can't allocate resources to process a packet
Explanation	The gateway ran out of resources when trying to allocate resources to send a packet. The packet that triggered the need to send a packet will be dropped.
Gateway Action	drop
Recommended Action	Check buffer consumption.
Revision	1

2.34.6. failed_to_send_ack (ID: 04800008)

Default Severity	ERROR
Log Message	Failed to send TCP ACK in response to a segment
Explanation	The gateway responds to some segments by sending an acknowledgement segment to the sender. An example is when it receives a segment that is outside of the receiver's receive window. This log message indicates that the gateway failed to allocate resources to send such an acknowledgement segment.
Gateway Action	none
Recommended Action	Check buffer consumption.
Revision	1

2.34.7. processing_memory_limit_reached (ID: 04800009)

Default Severity	NOTICE
------------------	--------

Log Message	Maximum processing memory limit reached
Explanation	The reassembly subsystem has reached the maximum limit set on its processing memory. This will decrease the performance of connections that are processed by the reassembly subsystem.
Gateway Action	drop
Recommended Action	Consider increasing the setting Reassembly_MaxProcessingMem.
Revision	1

2.34.8. maximum_connections_limit_reached (ID: 04800010)

Default Severity	NOTICE
Log Message	Maximum connections limit reached
Explanation	The reassembly subsystem has reached the maximum number of concurrent connections.
Gateway Action	none
Recommended Action	Consider increasing the setting Reassembly_MaxConnections.
Revision	1
Context Parameters	Connection

2.34.9. state_memory_allocation_failed (ID: 04800011)

Default Severity	ERROR
Log Message	Failed to allocate the memory needed to activate reassembly on a connection
Explanation	The reassembly subsystem has failed to allocate the memory needed to activate reassembly on a connection.
Gateway Action	none
Recommended Action	Review configuration to reduce memory consumption.
Revision	1
Context Parameters	Connection

2.35. RFO

These log messages refer to the **RFO (Route fail over events)** category.

2.35.1. has_ping (ID: 04100001)

Default Severity	NOTICE
Log Message	Interface <iface>, Table <table>, Net <net>: Route enabled, got PING reply from GW <gateway>
Explanation	Route is available. Received PING reply from the gateway.
Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	iface table net gateway

2.35.2. no_ping (ID: 04100002)

Default Severity	WARNING
Log Message	Interface <iface>, Table <table>, Net <net>: Unable to open conn for PING trying again later
Explanation	Unable to open a connection to verify the status of the route. Will try again later.
Gateway Action	try_again_later
Recommended Action	None.
Revision	1
Parameters	iface table net gateway

2.35.3. no_ping (ID: 04100003)

Default Severity	ERROR
Log Message	Interface <iface>, Table <table>, Net <net>: Route disabled, no PING reply from Gateway <gateway>
Explanation	Route is not available, and has been disabled. Did not receive a PING reply from the gateway.
Gateway Action	route_disabled

Recommended Action	None.
Revision	1
Parameters	iface table net gateway

2.35.4. unable_to_register_pingmon (ID: 04100004)

Default Severity	WARNING
Log Message	Interface <iface>, Table <table>, Net <net>: Route no longer monitored, unable to register PING monitor
Explanation	Internal Error: The route is no longer monitored. Failed to register PING Route Monitor.
Gateway Action	route_not_monitored
Recommended Action	None.
Revision	1
Parameters	iface table net gateway

2.35.5. unable_to_register_pingmon (ID: 04100005)

Default Severity	ERROR
Log Message	Interface <iface>, Table <table>, Net <net>: Route no longer monitored via PING, unable to register PING monitor
Explanation	Internal Error: The route is no longer monitored. Failed to register PING Route Monitor.
Gateway Action	disabled_monitor
Recommended Action	None.
Revision	1
Parameters	iface table net gateway

2.35.6. has_arp (ID: 04100006)

Default Severity	NOTICE
Log Message	Interface <iface>, Table <table>, Net <net>: Route enabled, got ARP

	reply from Gateway <gateway>
Explanation	Route is available. Received ARP reply from the gateway.
Gateway Action	route_enabled
Recommended Action	None.
Revision	2
Parameters	iface table net gateway

2.35.7. no_arp (ID: 04100007)

Default Severity	ERROR
Log Message	Interface <iface>, Table <table>, Net <net>: Route disabled, no ARP reply from Gateway <gateway>
Explanation	Route is not available, and has been disabled. Did not receive a ARP reply from the gateway.
Gateway Action	route_enabled
Recommended Action	None.
Revision	1
Parameters	iface table net gateway

2.35.8. unable_to_register_arp_monitor (ID: 04100008)

Default Severity	ERROR
Log Message	Interface <iface>, Table <table>, Net <net>: Route no longer monitored, unable to register ARP monitor
Explanation	Internal Error: The route is no longer monitored. Failed to register ARP Route Monitor.
Gateway Action	no_monitoring
Recommended Action	None.
Revision	1
Parameters	iface table net gateway

2.35.9. unable_to_register_arp_monitor (ID: 04100009)

Default Severity	WARNING
Log Message	Interface <iface>, Table <table>, Net <net>: Route no longer monitored via ARP, unable to register ARP monitor
Explanation	Internal Error: The route is no longer monitored. Failed to register ARP Route Monitor.
Gateway Action	disabled_monitor
Recommended Action	None.
Revision	1
Parameters	iface table net gateway

2.35.10. no_link (ID: 04100010)

Default Severity	ERROR
Log Message	Interface <iface> has no link (reason: <reason>), all associated routes disabled.
Explanation	The interface has no link, and all associated routes has been disabled.
Gateway Action	associated_routes_disabled
Recommended Action	None.
Revision	2
Parameters	iface reason

2.35.11. has_link (ID: 04100011)

Default Severity	NOTICE
Log Message	Interface <iface> has link. Some associated routes may require ARP to be enabled
Explanation	The interface has a link. Some associated routes may require ARP to be enabled.
Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	iface

2.35.12. unable_to_register_interface_monitor (ID:

04100012)

Default Severity	ERROR
Log Message	Interface <iface>, Table <table>, Net <net>: Route no longer monitored, unable to register interface monitor
Explanation	Internal Error: Route is no longer monitored. Unable to register Interface Monitor.
Gateway Action	no_monitoring
Recommended Action	None.
Revision	1
Parameters	iface table net gateway

2.35.13. unable_to_register_interface_monitor (ID: 04100013)

Default Severity	ERROR
Log Message	Interface <iface>, Table <table>, Net <net>: Route no longer monitored, unable to register interface monitor
Explanation	Internal Error: Route is no longer monitored. Unable to register Interface Monitor.
Gateway Action	disabled_monitor
Recommended Action	None.
Revision	1
Parameters	iface table net gateway

2.35.14. hostmon_failed (ID: 04100014)

Default Severity	NOTICE
Log Message	Interface <iface>, Table <table>, Net <net>: Route disabled, host monitoring failed
Explanation	Route is disabled. Host monitoring failed.
Gateway Action	route_disabled
Recommended Action	None.
Revision	1

Parameters	iface table net
-------------------	-----------------------

2.35.15. hostmon_successful (ID: 04100015)

Default Severity	NOTICE
Log Message	Interface <iface>, Table <table>, Net <net>: Route enabled, host monitoring successful
Explanation	Route is available. Host monitoring successful.
Gateway Action	route_enabled
Recommended Action	None.
Revision	1
Parameters	iface table net

2.36. RULE

These log messages refer to the **RULE (Events triggered by rules)** category.

2.36.1. ruleset_fwdfast (ID: 06000003)

Default Severity	NOTICE
Log Message	Packet statelessly forwarded (fwdfast)
Explanation	The packet matches a rule with a "fwdfast" action, and is statelessly forwarded.
Gateway Action	fwdfast
Recommended Action	None.
Revision	1
Context Parameters	Rule Information Packet Buffer

2.36.2. ip_verified_access (ID: 06000005)

Default Severity	NOTICE
Log Message	IP address verified according to ACCESS section
Explanation	The IP address was verified according to the ACCESS section.
Gateway Action	access_allow
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.36.3. block0net (ID: 06000010)

Default Severity	WARNING
Log Message	Destination address is the 0.* net. Dropping
Explanation	The destination address was the 0.* net, which is not allowed according to the configuration. The packet is dropped.
Gateway Action	drop
Recommended Action	Investigate why this traffic had the 0.* net as the destination.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.36.4. block0net (ID: 06000011)

Default Severity	WARNING
Log Message	Destination address is the 0.* net. Accepting
Explanation	The destination address was the 0.* net, which is allowed according to the configuration. The packet is accepted.
Gateway Action	accept
Recommended Action	If this type of traffic should be dropped, modify the "Settings" section in the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.36.5. block127net (ID: 06000012)

Default Severity	WARNING
Log Message	Destination address is the 127.* net. Dropping
Explanation	The destination address was the 127.* net, which is not allowed according to the configuration. The packet is dropped.
Gateway Action	drop
Recommended Action	Investigate why this traffic had the 127.* net as the destination.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.36.6. block127net (ID: 06000013)

Default Severity	WARNING
Log Message	Destination address is the 127.* net. Accepting
Explanation	The destination address was the 127.* net, which is allowed according to the configuration. The packet is accepted.
Gateway Action	accept
Recommended Action	If this type of traffic should be dropped, modify the "Settings" section in the configuration.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.36.7. directed_broadcasts (ID: 06000030)

Default Severity	NOTICE
Log Message	Packet directed to the broadcast address of the destination network. Forwarding
Explanation	The packet was directed to the broadcast address of the destination network, and the unit is configured to allow this.
Gateway Action	forward
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.36.8. directed_broadcasts (ID: 06000031)

Default Severity	NOTICE
Log Message	Packet directed to the broadcast address of the destination network. Dropping
Explanation	The packet was directed to the broadcast address of the destination network, and the unit is configured to disallow this.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name

2.36.9. unknown_vlanid (ID: 06000040)

Default Severity	WARNING
Log Message	Received VLAN packet with unknown tag <vlanid>. Dropping
Explanation	The unit received a VLAN packet with an unknown tag, and the packet is dropped.
Gateway Action	drop
Recommended Action	None.
Revision	2
Parameters	vlanid
Context Parameters	Rule Name Packet Buffer

2.36.10. ruleset_reject_packet (ID: 06000050)

Default Severity	WARNING
Log Message	Packet rejected by rule-set. Rejecting
Explanation	The rule-set is configured to rejected this packet.
Gateway Action	reject
Recommended Action	If this is not the intended behaviour, modify the rule-set.
Revision	1
Context Parameters	Rule Information Packet Buffer

2.36.11. ruleset_drop_packet (ID: 06000051)

Default Severity	WARNING
Log Message	Packet dropped by rule-set. Dropping
Explanation	The rule-set is configured to drop this packet.
Gateway Action	drop
Recommended Action	If this is not the intended behaviour, modify the rule-set.
Revision	1
Context Parameters	Rule Information Packet Buffer

2.36.12. unhandled_local (ID: 06000060)

Default Severity	NOTICE
Log Message	Allowed but unhandled packet to the firewall. Dropping
Explanation	A packet directed to the unit itself was received. The packet is allowed, but there is no matching state information for this packet. It is not part of any open connections, and will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.37. SESMGR

These log messages refer to the **SESMGR (Session Manager events)** category.

2.37.1. sesmgr_session_created (ID: 04900001)

Default Severity	NOTICE
Log Message	Session connected for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	New session created in Session Manager.
Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	user database ip type

2.37.2. sesmgr_session_denied (ID: 04900002)

Default Severity	WARNING
Log Message	New session denied for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	New session denied in Session Manager.
Gateway Action	remove_session
Recommended Action	Check settings for users.
Revision	1
Parameters	user database ip type

2.37.3. sesmgr_session_removed (ID: 04900003)

Default Severity	NOTICE
Log Message	Session disconnected for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	Session disconnected in Session Manager.
Gateway Action	none
Recommended Action	None.

Revision	1
Parameters	user database ip type

2.37.4. sesmgr_access_set (ID: 04900004)

Default Severity	NOTICE
Log Message	Access level changed to <access> for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	Access level has been changed for session.
Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	user access database ip type

2.37.5. sesmgr_session_timeout (ID: 04900005)

Default Severity	NOTICE
Log Message	Session has timed out for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	Session has timed out and will be removed.
Gateway Action	remove_session
Recommended Action	None.
Revision	1
Parameters	user database ip type

2.37.6. sesmgr_upload_denied (ID: 04900006)

Default Severity	NOTICE
Log Message	File upload connection denied for User: <user>. IP: <ip>. Type: <type>.
Explanation	Administrator session already active, file upload session denied.

Gateway Action	deny_upload
Recommended Action	Terminate administrator session and try again.
Revision	1
Parameters	user ip type

2.37.7. sesmgr_console_denied (ID: 04900007)

Default Severity	WARNING
Log Message	Could not create new console for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	Could not create new console, new session will be removed.
Gateway Action	remove_session
Recommended Action	Check maximum number of sessions and consoles.
Revision	1
Parameters	user database ip type

2.37.8. sesmgr_session_maximum_reached (ID: 04900008)

Default Severity	WARNING
Log Message	Maximum number of sessions reached
Explanation	Maximum number of sessions reached.
Gateway Action	deny_new_session
Recommended Action	Remove inactive sessions or increase maximum number of allowed sessions.
Revision	1

2.37.9. sesmgr_allocate_error (ID: 04900009)

Default Severity	EMERGENCY
Log Message	Could not allocate memory for new session
Explanation	Could not allocate memory for new session.
Gateway Action	none
Recommended Action	Check memory.

Revision 1

2.37.10. sesmgr_session_activate (ID: 04900010)

Default Severity NOTICE

Log Message Session has been activated for User: <user>. Database: <database>. IP: <ip>. Type: <type>.

Explanation Disabled session has been activated.

Gateway Action none

Recommended Action None.

Revision 1

Parameters user
database
ip
type

2.37.11. sesmgr_session_disabled (ID: 04900011)

Default Severity NOTICE

Log Message Session has been disabled for User: <user>. Database: <database>. IP: <ip>. Type: <type>.

Explanation Session has been disabled.

Gateway Action none

Recommended Action None.

Revision 1

Parameters user
database
ip
type

2.37.12. sesmgr_console_denied_init (ID: 04900012)

Default Severity ALERT

Log Message Could not create new console at initialization of Security Gateway for User: <user>. Database: <database>. IP: <ip>. Type: <type>.

Explanation Could not create new console at initialization of Security Gateway.

Gateway Action remove_session

Recommended Action Check maximum number of sessions and consoles.

Revision 1

Parameters	user database ip type
-------------------	--------------------------------

2.37.13. sesmgr_session_previous_removed (ID: 04900014)

Default Severity	NOTICE
Log Message	Previous session for User: <user> will be disconnected. Database: <database>. IP: <ip>. Type: <type>.
Explanation	Previous session will be disconnected, current session will be established in its stead.
Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	user database ip type

2.37.14. sesmgr_session_access_missing (ID: 04900015)

Default Severity	WARNING
Log Message	No access level set for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	No access level set for user, new session denied.
Gateway Action	deny_session
Recommended Action	Check user settings.
Revision	1
Parameters	user database ip type

2.37.15. sesmgr_session_old_removed (ID: 04900016)

Default Severity	NOTICE
Log Message	Old session disconnected to be replaced for User: <user>. Database: <database>. IP: <ip>. Type: <type>.
Explanation	Old session disconnected and is being replaced by a new session for the user.

Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	user database ip type

2.37.16. sesmgr_file_error (ID: 04900017)

Default Severity	ALERT
Log Message	Error accessing files.
Explanation	Error occurred when accessing files for reading/writing.
Gateway Action	file_error
Recommended Action	Check available memory.
Revision	1

2.37.17. sesmgr_techsupport (ID: 04900018)

Default Severity	NOTICE
Log Message	Sending technical support file.
Explanation	Technical support file created and is being sent to user.
Gateway Action	techsupport_created
Recommended Action	None.
Revision	1

2.38. SLB

These log messages refer to the **SLB (SLB events)** category.

2.38.1. server_online (ID: 02900001)

Default Severity	NOTICE
Log Message	SLB Server <server_ip> is online according to monitor
Explanation	A disabled server has been determined to be alive again.
Gateway Action	Adding this server to the active servers list.
Recommended Action	None.
Revision	1
Parameters	server_ip
Context Parameters	Rule Name

2.38.2. server_offline (ID: 02900002)

Default Severity	WARNING
Log Message	SLB Server <server_ip> is offline according to monitor
Explanation	The server is determined to be offline according to monitor.
Gateway Action	Removing this server from the active servers list.
Recommended Action	Determine why the server is not responding.
Revision	1
Parameters	server_ip [monitor] [monitor_port]
Context Parameters	Rule Name

2.39. SNMP

These log messages refer to the **SNMP (Allowed and disallowed SNMP accesses)** category.

2.39.1. disallowed_sender (ID: 03100001)

Default Severity	NOTICE
Log Message	Disallowed SNMP from <peer>, disallowed sender IP
Explanation	The sender IP address is not allowed to send SNMP data to the unit. Dropping packet.
Gateway Action	drop
Recommended Action	If this sender IP address should have SNMP access to the unit, this should be configured in the ACCESS section.
Revision	1
Parameters	peer
Context Parameters	Connection

2.39.2. invalid_snmp_community (ID: 03100002)

Default Severity	NOTICE
Log Message	Disallowed SNMP from <peer>, invalid community string
Explanation	The SNMP community string is invalid.
Gateway Action	drop
Recommended Action	Make sure the entered SNMP community string is correct.
Revision	1
Parameters	peer
Context Parameters	Connection

2.40. SYSTEM

These log messages refer to the **SYSTEM (System-wide events: startup, shutdown, etc.)** category.

2.40.1. demo_expired (ID: 03200020)

Default Severity	EMERGENCY
Log Message	The DEMO period for this copy of Clavister CorePlus has expired. Please install license and re-run Clavister CorePlus, or restart the firewall to initiate another evaluation session
Explanation	The unit will no longer operate, as the demo period has expired. Install a license in order to avoid this.
Gateway Action	shutdown
Recommended Action	Install a license.
Revision	1
Parameters	shutdown

2.40.2. demo_mode (ID: 03200021)

Default Severity	ALERT
Log Message	This copy of Clavister CorePlus is in DEMO mode. Firewall core will halt in <time> seconds
Explanation	The unit is running in DEMO mode, and will eventually expire. Install a license in order to avoid this.
Gateway Action	shutdown_soon
Recommended Action	Install a license.
Revision	1
Parameters	shutdown time

2.40.3. reset_clock (ID: 03200100)

Default Severity	NOTICE
Log Message	The clock at <oldtime> was manually reset by <user> to <newtime>
Explanation	The clock has manually been reset.
Gateway Action	None
Recommended Action	None.
Revision	1

Parameters	oldtime newtime user
-------------------	----------------------------

2.40.4. reset_clock (ID: 03200101)

Default Severity	NOTICE
Log Message	The clock at <oldtime> was manually reset to <newtime>
Explanation	The clock has manually been reset.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	oldtime newtime

2.40.5. invalid_ip_match_access_section (ID: 03200110)

Default Severity	WARNING
Log Message	Failed to verify IP address as per ACCESS section. Dropping
Explanation	The IP address was not verified according to the ACCESS section.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.40.6. port_bind_failed (ID: 03200300)

Default Severity	ALERT
Log Message	Out of memory while trying to allocate dynamic port for local IP <localip> to destination IP <destip>
Explanation	The unit failed to allocate a dynamic port, as it is out of memory.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason localip destip

2.40.7. port_bind_failed (ID: 03200301)

Default Severity	WARNING
Log Message	Out of dynamic assigned ports. All ports <port_base>-<port_end> for Local IP <localip> to Destination IP <destip> are in use
Explanation	Failed to allocate a dynamic port, as all ports are in use.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	reason localip destip port_base port_end

2.40.8. port_hlm_conversion (ID: 03200302)

Default Severity	NOTICE
Log Message	Using High Load Mode for Local IP <localip> Destination IP <destip> pair
Explanation	Mode for Local IP - Destination IP pair has changed to High Load because of heavy traffic.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	localip destip

2.40.9. port_llm_conversion (ID: 03200303)

Default Severity	NOTICE
Log Message	Using Low Load Mode for Local IP <localip> Destination IP <destip> pair
Explanation	Mode for Local IP - Destination IP pair has changed to Low Load because of low traffic.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	localip

destip

2.40.10. ssl_encryption_failed (ID: 03200450)

Default Severity	ERROR
Log Message	Encryption failed.
Explanation	Encryption failed due to error. Connection closed.
Gateway Action	None
Recommended Action	None.
Revision	1

2.40.11. bidir_fail (ID: 03200600)

Default Severity	CRITICAL
Log Message	Failed to establish bi-directional communication with peer in <timeout> seconds
Explanation	The unit failed to establish a connection back to peer, using the new configuration. It will try to revert to the previous configuration file.
Gateway Action	None
Recommended Action	Verify that the new configuration file does not contain errors that would cause bi-directional communication failure.
Revision	1
Parameters	cfgver timeout

2.40.12. disk_cannot_remove_file (ID: 03200601)

Default Severity	CRITICAL
Log Message	Failed to remove <file>, bi-directional communication will now probably be impossible
Explanation	The unit failed to remove the new, faulty, configuration file. It will still try to revert to the previous configuration file.
Gateway Action	None
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	file

2.40.13. file_open_failed (ID: 03200602)

Default Severity	ERROR
Log Message	Failed to open newly uploaded configuration file <new_cfg>
Explanation	The unit failed to open the uploaded configuration file.
Gateway Action	None
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	new_cfg

2.40.14. disk_cannot_remove (ID: 03200603)

Default Severity	ERROR
Log Message	Failed to remove <old_cfg>
Explanation	The unit failed to remove the old configuration file.
Gateway Action	None
Recommended Action	Verify that the disk media is intact, and that the file is not write protected.
Revision	1
Parameters	old_cfg

2.40.15. disk_cannot_rename (ID: 03200604)

Default Severity	ERROR
Log Message	Failed to rename <cfg_new> to <cfg_real>
Explanation	The unit failed to rename the new configuration file to the real configuration file name.
Gateway Action	None
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	cfg_new cfg_real

2.40.16. cfg_switch_fail (ID: 03200605)

Default Severity	CRITICAL
Log Message	Failed to switch to new configuration
Explanation	For reasons specified in earlier log events, the unit failed to switch to

	the new configuration and will continue to use the present configuration.
Gateway Action	None
Recommended Action	Consult the recommended action in the previous log message, which contained a more detailed error description.
Revision	1

2.40.17. core_switch_fail (ID: 03200606)

Default Severity	CRITICAL
Log Message	Failed to switch to new core
Explanation	For reasons specified in earlier log events, the unit failed to switch to the new core executable and will continue to use the present core executable.
Gateway Action	None
Recommended Action	Consult the recommended action in the previous log message, which contained a more detailed error description.
Revision	1

2.40.18. bidir_ok (ID: 03200607)

Default Severity	NOTICE
Log Message	Configuration <cfgver> verified for bi-directional communication
Explanation	The new configuration has been verified for communication back to peer, and will now be used as the active configuration.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	cfgver

2.40.19. shutdown (ID: 03201000)

Default Severity	NOTICE
Log Message	Shutdown <shutdown>. Active in <time> seconds. Reason: <reason>
Explanation	The unit is shutting down.
Gateway Action	shutdown
Recommended Action	None.
Revision	1

Parameters	shutdown time reason
-------------------	----------------------------

2.40.20. shutdown (ID: 03201010)

Default Severity	NOTICE
Log Message	Reconfiguration aborted. Configuration files are missing
Explanation	The unit was issued a reconfigure command, but no configuration file is seen. The reconfiguration process is aborted.
Gateway Action	reconfigure_gateway_aborted
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	reason

2.40.21. shutdown (ID: 03201011)

Default Severity	NOTICE
Log Message	Shutdown aborted. Core file <core> missing
Explanation	The unit was issued a shutdown command, but no core executable file is seen. The shutdown process is aborted.
Gateway Action	shutdown_gateway_aborted
Recommended Action	Verify that the disk media is intact.
Revision	1
Parameters	shutdown reason core

2.40.22. startup_normal (ID: 03202000)

Default Severity	NOTICE
Log Message	Security gateway starting. Core: <corever>. Build: <build>. Current uptime: <uptime>. Using configuration file <cfgfile>, version <cfgver>. Previous shutdown: <previous_shutdown>
Explanation	The Security Gateway is starting up.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	corever

build
 uptime
 cfgfile
 cfgver
 previous_shutdown

2.40.23. startup_echo (ID: 03202001)

Default Severity	NOTICE
Log Message	Security gateway starting echo (<delay> seconds). Core: <corever>. Build: <build>. Current uptime: <uptime>. Using configuration file <cfgfile>, version <cfgver>. Previous shutdown: <previous_shutdown>
Explanation	The Security Gateway is starting up, echo.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	delay corever build uptime cfgfile cfgver previous_shutdown

2.40.24. shutdown (ID: 03202500)

Default Severity	NOTICE
Log Message	Shutdown <shutdown>
Explanation	The Security Gateway is shutting down.
Gateway Action	shutdown
Recommended Action	None.
Revision	1
Parameters	shutdown

2.40.25. admin_login (ID: 03203000)

Default Severity	NOTICE
Log Message	Administrative user <username> logged in via <authsystem>. Access level: <access_level>
Explanation	An administrative user has logged in to the configuration system.

Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	authsystem username access_level [userdb] [server_ip] [server_port] [client_ip] [client_port]

2.40.26. admin_logout (ID: 03203001)

Default Severity	NOTICE
Log Message	Administrative user <username> logged out, via <authsystem>. Access level: <access_level>
Explanation	An administrative user has logged out from the configuration system.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	authsystem username access_level [userdb] [client_ip]

2.40.27. admin_login_failed (ID: 03203002)

Default Severity	WARNING
Log Message	Administrative user <username> failed to log in via <authsystem>, because of bad credentials
Explanation	An administrative user failed to log in to configuration system. This is most likely due to an invalid entered username or password.
Gateway Action	disallow_admin_access
Recommended Action	None.
Revision	1
Parameters	authsystem username [server_ip] [server_port] [client_ip] [client_port]

2.41. TCP_FLAG

These log messages refer to the **TCP_FLAG (Events concerning the TCP header flags)** category.

2.41.1. tcp_flags_set (ID: 03300001)

Default Severity	NOTICE
Log Message	The TCP <good_flag> and <bad_flag> flags are set. Allowing
Explanation	The possible combinations for these flags are: SYN URG, SYN PSH, SYN RST, SYN FIN and FIN URG.
Gateway Action	allow
Recommended Action	If any of these combinations should either be dropped or having the bad flag stripped, specify this in configuration, in the "Settings" sub system.
Revision	1
Parameters	good_flag bad_flag
Context Parameters	Rule Name Packet Buffer

2.41.2. tcp_flags_set (ID: 03300002)

Default Severity	WARNING
Log Message	The TCP <good_flag> and <bad_flag> flags are set. Stripping <bad_flag> flag
Explanation	The possible combinations for these flags are: SYN URG, SYN PSH, SYN RST, SYN FIN and FIN URG. Removing the "bad" flag.
Gateway Action	strip_bad_flag
Recommended Action	If any of these combinations should either be dropped or ignored, specify this in configuration, in the "Settings" sub system.
Revision	1
Parameters	good_flag bad_flag
Context Parameters	Rule Name Packet Buffer

2.41.3. tcp_flag_set (ID: 03300003)

Default Severity	NOTICE
Log Message	The TCP <bad_flag> flag is set. Ignoring
Explanation	The TCP flag is set. Ignoring.

Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	bad_flag
Context Parameters	Rule Name Packet Buffer

2.41.4. tcp_flag_set (ID: 03300004)

Default Severity	NOTICE
Log Message	The TCP <bad_flag> flag is set. Stripping
Explanation	A "bad" TCP flag is set. Removing it.
Gateway Action	strip_flag
Recommended Action	None.
Revision	1
Parameters	bad_flag
Context Parameters	Rule Name Packet Buffer

2.41.5. tcp_null_flags (ID: 03300005)

Default Severity	NOTICE
Log Message	Packet has no SYN, ACK, FIN or RST flag set
Explanation	The packet has no SYN, ACK, FIN or RST flag set. Ignoring.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.41.6. tcp_flags_set (ID: 03300008)

Default Severity	WARNING
Log Message	The TCP <good_flag> and <bad_flag> flags are set. Dropping
Explanation	The possible combinations for these flags are: SYN URG, SYN PSH, SYN RST, SYN FIN and FIN URG.
Gateway Action	drop

Recommended Action	If any of these combinations should either be ignored or having the bad flag stripped, specify this in configuration, in the "Settings" sub system.
Revision	1
Parameters	good_flag bad_flag
Context Parameters	Rule Name Packet Buffer

2.41.7. tcp_flag_set (ID: 03300009)

Default Severity	WARNING
Log Message	The TCP <bad_flag> flag is set. Dropping
Explanation	The TCP flag is set. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	bad_flag
Context Parameters	Rule Name Packet Buffer

2.41.8. unexpected_tcp_flags (ID: 03300010)

Default Severity	WARNING
Log Message	Unexpected tcp flags <flags> from <endpoint> during state <state>. Dropping
Explanation	Received unexpected tcp flags during a specific state. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	flags endpoint state
Context Parameters	Rule Name Connection Packet Buffer

2.41.9. mismatched_syn_resent (ID: 03300011)

Default Severity	WARNING
Log Message	Mismatched syn "resent" with seq <seqno>, expected <origseqno>. Dropping
Explanation	Mismatching sequence numbers. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno origseqno
Context Parameters	Rule Name Connection Packet Buffer

2.41.10. mismatched_first_ack_seqno (ID: 03300012)

Default Severity	WARNING
Log Message	ACK packet with seq <seqno>. Expected <expectseqno>. Dropping
Explanation	Mismatching sequence numbers. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno expectseqno
Context Parameters	Rule Name Connection Packet Buffer

2.41.11. mismatched_first_ack_seqno (ID: 03300013)

Default Severity	WARNING
Log Message	SYNACK packet with seq <seqno>. Expected <expectseqno>. Dropping
Explanation	Mismatching sequence numbers. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno expectseqno

Context Parameters	Rule Name Connection Packet Buffer
---------------------------	--

2.41.12. rst_out_of_bounds (ID: 03300015)

Default Severity	WARNING
Log Message	Originator RST seq <seqno> is not in window <winstart>...<winend>. Dropping
Explanation	The RST flag sequence number is not within the receiver window. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno winstart winend
Context Parameters	Rule Name Connection Packet Buffer

2.41.13. tcp_seqno_too_low (ID: 03300016)

Default Severity	DEBUG
Log Message	TCP sequence number <seqno> is not in the acceptable range <accstart>-<accend>. Dropping
Explanation	A TCP segment with an unacceptable sequence number was received. The packet will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	2
Parameters	seqno accstart accend
Context Parameters	Rule Name Connection Packet Buffer

2.41.14. unacceptable_ack (ID: 03300017)

Default Severity	NOTICE
-------------------------	--------

Log Message	TCP acknowledgement <ack> is not in the acceptable range <accstart>-<accend>. Dropping
Explanation	A TCP segment with an unacceptable acknowledgement number was received during state SYN_SENT. The packet will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	ack accstart accend
Context Parameters	Rule Name Connection Packet Buffer

2.41.15. rst_without_ack (ID: 03300018)

Default Severity	NOTICE
Log Message	TCP RST segment without ACK during state SYN_SENT. Dropping
Explanation	A TCP segment with the RST flag but not the ACK flag was received during state SYN_SENT. The packet will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Connection Packet Buffer

2.41.16. tcp_seqno_too_high (ID: 03300019)

Default Severity	WARNING
Log Message	TCP sequence number <seqno> is not in the acceptable range <accstart>-<accend>. Dropping
Explanation	A TCP segment with an unacceptable sequence number was received. The packet will be dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	seqno accstart accend

Context Parameters	Rule Name Connection Packet Buffer
---------------------------	--

2.41.17. tcp_rcv_windows_drained (ID: 03300022)

Default Severity	CRITICAL
Log Message	Out of large TCP receive windows. Maximum windows: <max_windows>. Triggered <num_events> times last 10 seconds.
Explanation	The TCP stack could not accept incoming data since it has run out of large TCP receive windows. This event was triggered [num_events] times during the last 10 seconds.
Gateway Action	close
Recommended Action	If the system is configured to use TCP based ALGs, increase the amount of maximum sessions parameter on the associated service.
Revision	1
Parameters	max_windows [num_events]

2.41.18. tcp_snd_windows_drained (ID: 03300023)

Default Severity	CRITICAL
Log Message	Out of large TCP send windows. Maximum windows: <max_windows>. Triggered <num_events> times last 10 seconds.
Explanation	The TCP stack could not send data since it has run out of large TCP send windows. This event was triggered [num_events] times during the last 10 seconds.
Gateway Action	close
Recommended Action	If the system is configured to use TCP based ALGs, increase the amount of maximum sessions parameter on the associated service.
Revision	1
Parameters	max_windows [num_events]

2.41.19. tcp_get_freesocket_failed (ID: 03300024)

Default Severity	WARNING
Log Message	System was not able to get a free socket. Triggered <num_events> times last 10 seconds.
Explanation	The TCP stack could not get a free socket. This event was triggered [num_events] times during the last 10 seconds.

Gateway Action	None
Recommended Action	None.
Revision	1

2.42. TCP_OPT

These log messages refer to the **TCP_OPT (Events concerning the TCP header options)** category.

2.42.1. tcp_mss_too_low (ID: 03400001)

Default Severity	NOTICE
Log Message	TCP MSS <mss> too low. TCPMSSMin=<minmss>
Explanation	The TCP MSS is too low. Ignoring.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	tcpopt mss minmss
Context Parameters	Rule Name Packet Buffer

2.42.2. tcp_mss_too_low (ID: 03400002)

Default Severity	NOTICE
Log Message	TCP MSS <mss> too low. TCPMSSMin=<minmss>. Adjusting
Explanation	The TCP MSS is too low. Adjusting to use the configured minimum MSS.
Gateway Action	adjust
Recommended Action	None.
Revision	1
Parameters	tcpopt mss minmss
Context Parameters	Rule Name Packet Buffer

2.42.3. tcp_mss_too_high (ID: 03400003)

Default Severity	NOTICE
Log Message	TCP MSS <mss> too high. TCPMSSMax=<maxmss>
Explanation	The TCP MSS is too high. Ignoring.
Gateway Action	None

Recommended Action	None.
Revision	1
Parameters	tcpopt mss maxmss
Context Parameters	Rule Name Packet Buffer

2.42.4. tcp_mss_too_high (ID: 03400004)

Default Severity	NOTICE
Log Message	TCP MSS <mss> too high. TCPMSSMax=<maxmss>. Adjusting
Explanation	The TCP MSS is too high. Adjusting to use the configured maximum MSS.
Gateway Action	adjust
Recommended Action	None.
Revision	1
Parameters	tcpopt mss maxmss
Context Parameters	Rule Name Packet Buffer

2.42.5. tcp_mss_above_log_level (ID: 03400005)

Default Severity	NOTICE
Log Message	TCP MSS <mss> higher than log level. TCPMSSLogLevel=<mssloglevel>
Explanation	The TCP MSS is higher than the log level.
Gateway Action	log
Recommended Action	None.
Revision	1
Parameters	tcpopt mss mssloglevel
Context Parameters	Rule Name Packet Buffer

2.42.6. tcp_option (ID: 03400006)

Default Severity	NOTICE
Log Message	Packet has a type <tcpopt> TCP option
Explanation	The packet has a TCP Option of the specified type. Ignoring.
Gateway Action	ignore
Recommended Action	None.
Revision	1
Parameters	tcpopt
Context Parameters	Rule Name Packet Buffer

2.42.7. tcp_option_strip (ID: 03400007)

Default Severity	NOTICE
Log Message	Packet has a type <tcpopt> TCP option. Stripping it
Explanation	The packet has a TCP Option of the specified type. Removing it.
Gateway Action	strip
Recommended Action	None.
Revision	1
Parameters	tcpopt
Context Parameters	Rule Name Packet Buffer

2.42.8. bad_tcpopt_length (ID: 03400010)

Default Severity	WARNING
Log Message	Type <tcpopt> is multibyte, available=<avail>. Dropping
Explanation	The TCP Option type is multi byte which requires two bytes, and there is less than two bytes available. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	tcpopt minoptlen avail
Context Parameters	Rule Name Packet Buffer

2.42.9. bad_tcptopt_length (ID: 03400011)

Default Severity	WARNING
Log Message	Type <tcptopt> claims length=<len> bytes, avail=<avail> bytes. Dropping
Explanation	The TCP Option type does not fit in the option space. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	tcptopt len avail
Context Parameters	Rule Name Packet Buffer

2.42.10. bad_tcptopt_length (ID: 03400012)

Default Severity	WARNING
Log Message	Type <tcptopt>: bad length <optlen>. Expected <expectlen> bytes. Dropping
Explanation	The TCP Option type has an invalid length. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	tcptopt optlen expectlen
Context Parameters	Rule Name Packet Buffer

2.42.11. tcp_mss_too_low (ID: 03400013)

Default Severity	WARNING
Log Message	TCP MSS <mss> too low. TCPMSSMin=<minmss>. Dropping
Explanation	The TCP MSS is too low. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1

Parameters	tcpopt mss minmss
Context Parameters	Rule Name Packet Buffer

2.42.12. tcp_mss_too_high (ID: 03400014)

Default Severity	WARNING
Log Message	TCP MSS <mss> too high. TCPMSSMax=<maxmss>. Dropping
Explanation	The TCP MSS is too high. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	tcpopt mss maxmss
Context Parameters	Rule Name Packet Buffer

2.42.13. tcp_option_disallowed (ID: 03400015)

Default Severity	WARNING
Log Message	Packet has a <tcpopt> TCP option, which is disallowed. Dropping
Explanation	The packet has a TCP Option of the specified type. Dropping packet.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	tcpopt
Context Parameters	Rule Name Packet Buffer

2.42.14. tcp_null_flags (ID: 03400016)

Default Severity	WARNING
Log Message	Packet has no SYN, ACK, FIN or RST flag set. Dropping
Explanation	The packet has no SYN, ACK, FIN or RST flag set. Dropping packet.
Gateway Action	drop

Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.42.15. multiple_tcp_ws_options (ID: 03400017)

Default Severity	WARNING
Log Message	Multiple window scale options present in a single TCP segment
Explanation	Multiple TCP window scale options present in a single TCP segment.
Gateway Action	strip
Recommended Action	None.
Revision	1
Context Parameters	Connection Packet Buffer

2.42.16. too_large_tcp_window_scale (ID: 03400018)

Default Severity	WARNING
Log Message	TCP window scale option with shift count <shift_cnt> was received. The shift count will be lowered to 14.
Explanation	A TCP segment with a window scale option specifying a shift count that is larger than 14 was received. The shift count will be lowered to 14.
Gateway Action	adjust
Recommended Action	None.
Revision	1
Parameters	shift_cnt
Context Parameters	Connection Packet Buffer

2.42.17. mismatching_tcp_window_scale (ID: 03400019)

Default Severity	WARNING
Log Message	Mismatching TCP window scale shift count. Expected <old> got <new> will use <effective>
Explanation	TCP segment with a window scale option specifying a different shift count than previous segments was received. The lower of the two values will be used.

Gateway Action	adjust
Recommended Action	None.
Revision	1
Parameters	old new effective
Context Parameters	Connection Packet Buffer

2.43. THRESHOLD

These log messages refer to the **THRESHOLD (Threshold rule events)** category.

2.43.1. conn_threshold_exceeded (ID: 05300100)

Default Severity	WARNING
Log Message	Connection threshold <description> exceeded <threshold>. Source IP: <srcip>. Closing connection
Explanation	The source ip is opening up new connections too fast.
Gateway Action	closing_connection
Recommended Action	Investigate worms and DoS attacks.
Revision	1
Parameters	description threshold srcip
Context Parameters	Rule Name

2.43.2. reminder_conn_threshold (ID: 05300101)

Default Severity	INFORMATIONAL
Log Message	Reminder: Connection threshold <description> exceeded <threshold>. Source IP: <srcip>.
Explanation	The source ip is still opening up new connections too fast.
Gateway Action	None
Recommended Action	Look through logs to see if the source ip has misbehaved in the past.
Revision	1
Parameters	description threshold srcip
Context Parameters	Rule Name

2.43.3. conn_threshold_exceeded (ID: 05300102)

Default Severity	NOTICE
Log Message	Connection threshold <description> exceeded <threshold>. Source IP: <srcip>
Explanation	The source ip is opening up new connections too fast.
Gateway Action	None

Recommended Action	Investigate worms and DoS attacks.
Revision	1
Parameters	description threshold srcip
Context Parameters	Rule Name

2.43.4. failed_to_keep_connection_count (ID: 05300200)

Default Severity	ERROR
Log Message	Failed to keep connection count. Reason: Out of memory
Explanation	The device was unable to allocate resources needed to include the connection in the connection count kept by threshold rules. The connection will not be included in the connection count.
Gateway Action	none
Recommended Action	Check memory consumption.
Revision	1
Context Parameters	Connection

2.43.5. failed_to_keep_connection_count (ID: 05300201)

Default Severity	ERROR
Log Message	Failed to keep connection count. Reason: Out of memory
Explanation	The device was unable to allocate resources needed to include the connection in the connection count kept by threshold rules. Since there exist protect actions that are triggered by thresholds on the number of connections, the connection will be closed.
Gateway Action	close
Recommended Action	Check memory consumption.
Revision	1
Context Parameters	Connection

2.43.6. threshold_conns_from_srcip_exceeded (ID: 05300210)

Default Severity	NOTICE
Log Message	The number of connections matching the rule and originating from <srcip> exceeds <threshold>.
Explanation	The number of connections matching the threshold rule and originating

from a single host exceeds the configured threshold. Note: This log message is rate limited via an exponential back-off procedure.

Gateway Action	none
Recommended Action	None.
Revision	1
Parameters	threshold srcip [username]
Context Parameters	Rule Name

2.43.7. threshold_conns_from_srcip_exceeded (ID: 05300211)

Default Severity	NOTICE
Log Message	The number of connections matching the rule and originating from <srcip> exceeds <threshold>.
Explanation	The number of connections matching the threshold rule and originating from a single host exceeds the configured threshold. The configured protective measures will be triggered. Note: This log message is rate limited via an exponential back-off procedure.
Gateway Action	protect
Recommended Action	None.
Revision	1
Parameters	threshold srcip [username]
Context Parameters	Rule Name

2.43.8. threshold_conns_from_filter_exceeded (ID: 05300212)

Default Severity	NOTICE
Log Message	The number of connections matching the rule exceeds <threshold>. The Offending host is <srcip>.
Explanation	The number of connections matching the threshold rule exceeds the configured threshold. Note: This log message is rate limited via an exponential back-off procedure.
Gateway Action	none
Recommended Action	None.
Revision	1

Parameters	threshold srcip [username]
Context Parameters	Rule Name

2.43.9. threshold_conns_from_filter_exceeded (ID: 05300213)

Default Severity	NOTICE
Log Message	The number of connections matching the rule exceeds <threshold>. The Offending host is <srcip>.
Explanation	The number of connections matching the threshold rule exceeds the configured threshold. The configured protective measures will be triggered. Note: This log message is rate limited via an exponential back-off procedure.
Gateway Action	protect
Recommended Action	None.
Revision	1
Parameters	threshold srcip [username]
Context Parameters	Rule Name

2.44. TIMESYNC

These log messages refer to the **TIMESYNC (Firewall time synchronization events)** category.

2.44.1. synced_clock (ID: 03500001)

Default Severity	NOTICE
Log Message	The clock at <oldtime>, was off by <clockdrift> second(s) and synchronized with <timeserver> to <newtime>
Explanation	The clock has been synchronized with the time server.
Gateway Action	None
Recommended Action	None.
Revision	2
Parameters	oldtime newtime clockdrift timeserver

2.44.2. failure_communicate_with_timeservers (ID: 03500002)

Default Severity	WARNING
Log Message	Communication with the timeserver(s) failed. Clock not updated.
Explanation	The unit failed to establish a connection with the time sync server. The clock has not been updated.
Gateway Action	clock_not_synced
Recommended Action	Verify that the time sync server is running.
Revision	1

2.44.3. clockdrift_too_high (ID: 03500003)

Default Severity	WARNING
Log Message	According to the timeserver the clock has drifted <clockdrift> seconds(s) which is NOT in the allowed correction interval (+/-<interval> seconds)
Explanation	The clock has drifted so much that it is not within the allowed +/- correction interval. The clock will not be updated.
Gateway Action	clock_not_synced
Recommended Action	If the correction interval is too narrow, it can be changed in the Advanced Settings section.

Revision	1
Parameters	clockdrift timeserver interval

2.45. TRANSPARENCY

These log messages refer to the **TRANSPARENCY (Events concerning the Transparent Mode feature)** category.

2.45.1. impossible_hw_sender_address (ID: 04400410)

Default Severity	WARNING
Log Message	Impossible hardware sender address 0000:0000:0000. Dropping.
Explanation	Some equipment on the network is sending packets with a source MAC address of 0000:0000:0000. These packets will be dropped.
Gateway Action	drop
Recommended Action	Investigate if there are equipment sending packets using 0000:0000:0000 as source MAC address. If there are, try to change the behaviour of that equipment.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.45.2. enet_hw_sender_broadcast (ID: 04400411)

Default Severity	NOTICE
Log Message	Ethernet hardware sender is a broadcast address. Accepting.
Explanation	The Ethernet hardware sender address is a broadcast address. The packet will be accepted.
Gateway Action	accept
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.45.3. enet_hw_sender_broadcast (ID: 04400412)

Default Severity	NOTICE
Log Message	Ethernet hardware sender is a broadcast address. Rewriting to the address of the forwarding interface.
Explanation	The Ethernet hardware sender address is a broadcast address. The packet will be rewritten with the hardware sender address of the forwarding interface.
Gateway Action	rewrite
Recommended Action	None.

Revision	1
Context Parameters	Rule Name Packet Buffer

2.45.4. enet_hw_sender_broadcast (ID: 04400413)

Default Severity	WARNING
Log Message	Ethernet hardware sender is a broadcast address. Dropping.
Explanation	The Ethernet hardware sender address is a broadcast address. The packet will be dropped.
Gateway Action	drop
Recommended Action	Investigate if there are equipment sending packets using a broadcast address as sender MAC address. If there are, try to change the behaviour of that equipment.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.45.5. enet_hw_sender_multicast (ID: 04400414)

Default Severity	NOTICE
Log Message	Ethernet hardware sender is a multicast address. Accepting.
Explanation	The Ethernet hardware sender address is a multicast address. The packet will be accepted.
Gateway Action	accept
Recommended Action	None.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.45.6. enet_hw_sender_multicast (ID: 04400415)

Default Severity	NOTICE
Log Message	Ethernet hardware sender is a multicast address. Rewriting to the address of the forwarding interface.
Explanation	The Ethernet hardware sender address is a multicast address. The packet will be rewritten with the hardware sender address of the forwarding interface.
Gateway Action	rewrite
Recommended Action	None.

Revision	1
Context Parameters	Rule Name Packet Buffer

2.45.7. enet_hw_sender_multicast (ID: 04400416)

Default Severity	WARNING
Log Message	Ethernet hardware sender is a multicast address. Dropping.
Explanation	The Ethernet hardware sender address is a multicast address. The packet will be dropped.
Gateway Action	drop
Recommended Action	Investigate if there are equipment sending packets using a multicast address as sender MAC address. If there are, try to change the behaviour of that equipment.
Revision	1
Context Parameters	Rule Name Packet Buffer

2.45.8. relay_stp_frame (ID: 04400417)

Default Severity	INFORMATIONAL
Log Message	Relaying STP frame from <recvif> to switched interfaces
Explanation	An incoming STP frame has been relayed to all switched interfaces in the same switch route as [recif].
Gateway Action	allow
Recommended Action	None.
Revision	1
Parameters	recvif

2.45.9. dropped_stp_frame (ID: 04400418)

Default Severity	INFORMATIONAL
Log Message	Dropping STP frame from <recvif>
Explanation	An incoming STP frame has been dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	recvif

2.45.10. invalid_stp_frame (ID: 04400419)

Default Severity	WARNING
Log Message	Incomming STP frame from <recvif> dropped. Reason: <reason>
Explanation	An incomming Spanning-Tree frame has been dropped since it is either malformed or its type is unknown. Supported Spanning-Tree versions are STP, RSTP, MSTP and PVST+.
Gateway Action	drop
Recommended Action	If the frame format is invalid, locate the unit which is sending the malformed frame.
Revision	1
Parameters	recvif reason

2.45.11. relay_mpls_frame (ID: 04400420)

Default Severity	INFORMATIONAL
Log Message	Forwarding MPLS packet from <recvif>.
Explanation	An incomming MPLS packet has been forwarded through the gateway. [destif] indicates if it was forwarded to an ultimate destination or if it was broadcasted to over all interfaces in the switch group.
Gateway Action	allow
Recommended Action	None.
Revision	1
Parameters	recvif destif

2.45.12. dropped_mpls_packet (ID: 04400421)

Default Severity	INFORMATIONAL
Log Message	Dropping MPLS packet from <recvif>
Explanation	An incomming MPLS packet has been dropped.
Gateway Action	drop
Recommended Action	None.
Revision	1
Parameters	recvif

2.45.13. invalid_mpls_packet (ID: 04400422)

Default Severity	WARNING
Log Message	Incomming MPLS packet on <recvif> dropped. Reason: <reason>
Explanation	An incomming MPLS packet has been dropped since it was malformed.
Gateway Action	drop
Recommended Action	If the packet format is invalid, locate the unit which is sending the malformed packet.
Revision	1
Parameters	recvif reason

2.46. USERAUTH

These log messages refer to the **USERAUTH (User authentication (e.g. RADIUS) events)** category.

2.46.1. accounting_start (ID: 03700001)

Default Severity	INFORMATIONAL
Log Message	Successfully received RADIUS Accounting START response from RADIUS Accounting server
Explanation	The unit received a valid response to an Accounting-Start event from the Accounting Server.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.46.2. invalid_accounting_start_server_response (ID: 03700002)

Default Severity	WARNING
Log Message	Received a RADIUS Accounting START response with an Identifier mismatch. Ignoring this packet
Explanation	The unit received a response with an invalid Identifier mismatch. This can be the result of a busy network, causing accounting event re-sends. This will be ignored.
Gateway Action	ignore_packet
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.46.3. no_accounting_start_server_response (ID: 03700003)

Default Severity	ALERT
Log Message	Did not receive a RADIUS Accounting START response. Accounting has been disabled
Explanation	The unit did not receive a response to an Accounting-Start event from the Accounting Server. Accounting features will be disabled.
Gateway Action	accounting_disabled

Recommended Action	Verify that the RADIUS Accounting server daemon is running on the Accounting Server.
Revision	1
Context Parameters	User Authentication

2.46.4. invalid_accounting_start_server_response (ID: 03700004)

Default Severity	ALERT
Log Message	Received an invalid RADIUS Accounting START response from RADIUS Accounting server. Accounting has been disabled
Explanation	The unit received an invalid response to an Accounting-Start event from the Accounting Server Accounting features will be disabled.
Gateway Action	accounting_disabled
Recommended Action	Verify that the RADIUS Accounting server is properly configured.
Revision	1
Context Parameters	User Authentication

2.46.5. no_accounting_start_server_response (ID: 03700005)

Default Severity	WARNING
Log Message	Logging out the authenticated user, as no RADIUS Accounting START response was received from RADIUS Accounting server
Explanation	The authenticated user is logged out as no response to the Accounting-Start event was received from the Accounting Server.
Gateway Action	logout_user
Recommended Action	Verify that the RADIUS Accounting server daemon is running on the Accounting Server.
Revision	1
Context Parameters	User Authentication

2.46.6. invalid_accounting_start_server_response (ID: 03700006)

Default Severity	WARNING
Log Message	Logging out the authenticated user, as an invalid RADIUS Accounting START response was received from RADIUS Accounting server
Explanation	The authenticated user is logged out as an invalid response to the

	Accounting-Start event was received from the Accounting Server.
Gateway Action	logout_user
Recommended Action	Verify that the RADIUS Accounting server is properly configured.
Revision	1
Context Parameters	User Authentication

2.46.7. failed_to_send_accounting_stop (ID: 03700007)

Default Severity	ALERT
Log Message	Failed to send Accounting STOP to Authentication Server. Accounting information will not be sent to Authentication Server.
Explanation	The unit failed to send an Accounting-Stop event to the Accounting Server. Accounting information will not be sent to the Accounting Server.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.46.8. accounting_stop (ID: 03700008)

Default Severity	NOTICE
Log Message	Successfully received RADIUS Accounting STOP response from RADIUS Accounting server. Bytes sent=<bytessent>, Bytes rcv=<bytesrcv>, Packets sent=<packetsent>, Packets rcv=<packetsrcv>, Session time=<sestime>
Explanation	The unit received a valid response to an Accounting-Stop event from the Accounting Server.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	bytessent bytesrcv packetsent packetsrcv gigawrapresent gigawraprecv sestime
Context Parameters	User Authentication

2.46.9. invalid_accounting_stop_server_response (ID:

03700009)

Default Severity	WARNING
Log Message	Received a RADIUS Accounting STOP response with an Identifier mismatch. Ignoring this packet
Explanation	The unit received a response with an invalid Identifier mismatch. This can be the result of a busy network, causing accounting event re-sends. This will be ignored.
Gateway Action	ignore_packet
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.46.10. no_accounting_stop_server_response (ID: 03700010)

Default Severity	ALERT
Log Message	Did not receive a RADIUS Accounting STOP response. User statistics might not have been updated on the Accounting Server
Explanation	The unit did not receive a response to an Accounting-Stop event from the Accounting Server. Accounting information might not have been properly received by the Accounting Server.
Gateway Action	None
Recommended Action	Verify that the RADIUS Accounting server daemon is running on the Accounting Server.
Revision	1
Context Parameters	User Authentication

2.46.11. invalid_accounting_stop_server_response (ID: 03700011)

Default Severity	ALERT
Log Message	Received an invalid RADIUS Accounting STOP response from RADIUS Accounting server. User statistics might not have been updated on the Accounting Server
Explanation	The unit received an invalid response to an Accounting-Stop event from the Accounting Server. Accounting information might not have been properly received by the Accounting Server.
Gateway Action	None
Recommended Action	Verify that the RADIUS Accounting server is properly configured.

Revision	1
Context Parameters	User Authentication

2.46.12. failure_init_radius_accounting (ID: 03700012)

Default Severity	ALERT
Log Message	Failed to send Accounting Start to RADIUS Accounting Server. Accounting will be disabled
Explanation	The unit failed to send an Accounting-Start event to the Accounting Server. Accounting features will be disabled.
Gateway Action	accounting_disabled
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.46.13. invalid_accounting_start_request (ID: 03700013)

Default Severity	WARNING
Log Message	Logging out the authenticated user, as a RADIUS Accounting START request could not be sent to the RADIUS Accounting server
Explanation	The authenticated user is logged out as an Accounting-Start request did not get sent to the Accounting Server. This could be a result of missing a route from the unit to the Accounting Server.
Gateway Action	logout_user
Recommended Action	Verify that a route exists from the unit to the RADIUS Accounting server, and that it is properly configured.
Revision	1
Context Parameters	User Authentication

2.46.14. no_accounting_start_server_response (ID: 03700014)

Default Severity	ALERT
Log Message	Did not send a RADIUS Accounting START request. Accounting has been disabled
Explanation	The unit did not send an Accounting-Start event to the Accounting Server. Accounting features will be disabled. This could be a result of missing a route from the unit to the Accounting Server.
Gateway Action	accounting_disabled

Recommended Action	Verify that a route exists from the unit to the RADIUS Accounting server, and that it is properly configured.
Revision	1
Context Parameters	User Authentication

2.46.15. user_timeout (ID: 03700020)

Default Severity	NOTICE
Log Message	User timeout expired, user is automatically logged out
Explanation	The user is automatically logged out, as the configured timeout expired.
Gateway Action	user_removed
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.46.16. group_list_too_long (ID: 03700030)

Default Severity	WARNING
Log Message	User <username> belongs in too many groups, keeping the 32 first groups
Explanation	A username can only be a member of a maximum of 32 groups. This username is a member of too many groups, and only the 32 first groups will be used.
Gateway Action	truncating_group_list
Recommended Action	Lower the number of groups that this user belongs to.
Revision	1
Parameters	username

2.46.17. accounting_alive (ID: 03700050)

Default Severity	NOTICE
Log Message	Successfully received RADIUS Accounting Interim response from RADIUS Accounting server. Bytes sent=<bytessent>, Bytes rcv=<bytesrcv>, Packets sent=<packetssent>, Packets rcv=<packetsrcv>, Session time=<sestime>
Explanation	The unit successfully received a RADIUS Accounting Interim response to an Accounting-Interim request event from the Accounting Server. Accounting information has been updated on the Accounting Server.

Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	bytessent bytesrecv packetsent packetsrecv gigawrapresent gigawraprecv sestime
Context Parameters	User Authentication

2.46.18. accounting_interim_failure (ID: 03700051)

Default Severity	ALERT
Log Message	Failed to send Accounting Interim to Authentication Server. Accounting information might not be properly updated on the Accounting Server.
Explanation	The unit failed to send an Accounting-Interim event to the Accounting Server. The statistics on the Accounting Server might not have been properly synchronized.
Gateway Action	None
Recommended Action	Verify that the RADIUS Accounting server daemon is running on the Accounting Server.
Revision	1
Context Parameters	User Authentication

2.46.19. no_accounting_interim_server_response (ID: 03700052)

Default Severity	ALERT
Log Message	Did not receive a RADIUS Accounting Interim response. User statistics might not have been updated on the Accounting Server
Explanation	The unit did not receive a response to an Accounting-Interim event from the Accounting Server. Accounting information might not have been properly received by the Accounting Server.
Gateway Action	None
Recommended Action	Verify that the RADIUS Accounting server daemon is running on the Accounting Server.
Revision	1
Context Parameters	User Authentication

2.46.20. invalid_accounting_interim_server_response (ID: 03700053)

Default Severity	ALERT
Log Message	Received an invalid RADIUS Accounting Interim response from RADIUS Accounting server. User statistics might not have been updated on the Accounting Server
Explanation	The unit received an invalid response to an Accounting-Interim event from the Accounting Server. Accounting information might not have been properly received by the Accounting Server.
Gateway Action	None
Recommended Action	Verify that the RADIUS Accounting server is properly configured.
Revision	1
Context Parameters	User Authentication

2.46.21. invalid_accounting_interim_server_response (ID: 03700054)

Default Severity	WARNING
Log Message	Received a RADIUS Accounting Interim response with an Identifier mismatch. Ignoring this packet
Explanation	The unit received a response with an invalid Identifier mismatch. This can be the result of a busy network, causing accounting event re-sends. This will be ignored.
Gateway Action	ignore_packet
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.46.22. relogin_from_new_srcip (ID: 03700100)

Default Severity	WARNING
Log Message	User with the same username is logging in from another IP address, logging out current instance
Explanation	A user with the same username as an already authenticated user is logging in. The current instance is logged out.
Gateway Action	logout_current_user
Recommended Action	None.
Revision	1

Context Parameters User Authentication

2.46.23. already_logged_in (ID: 03700101)

Default Severity	WARNING
Log Message	This user is already logged in
Explanation	A user with the same username as an already authenticated user tried to logged in, and was rejected .
Gateway Action	disallowed_login
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.46.24. user_login (ID: 03700102)

Default Severity	NOTICE
Log Message	User logged in. Idle timeout: <idle_timeout>, Session timeout: <session_timeout>
Explanation	A user logged in and has been granted access, according to the group membership or user name information.
Gateway Action	None
Recommended Action	None.
Revision	1
Parameters	idle_timeout session_timeout [groups]
Context Parameters	User Authentication

2.46.25. bad_user_credentials (ID: 03700104)

Default Severity	NOTICE
Log Message	Unknown user or invalid password
Explanation	A user failed to log in. The entered username or password was invalid.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.46.26. radius_auth_timeout (ID: 03700105)

Default Severity	ALERT
Log Message	Timeout during RADIUS user authentication, contact with RADIUS server not established
Explanation	The unit did not receive a response from the RADIUS Authentication server, and the authentication process failed.
Gateway Action	None
Recommended Action	Verify that the RADIUS Authentication server daemon is running on the Authentication Server.
Revision	1
Context Parameters	User Authentication

2.46.27. manual_logout (ID: 03700106)

Default Severity	NOTICE
Log Message	User manually logged out
Explanation	A user manually logged out, and is no longer authenticated.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.46.28. userauthrules_disallowed (ID: 03700107)

Default Severity	WARNING
Log Message	Denied access according to UserAuthRules rule-set
Explanation	The user is not allowed to authenticate according to the UserAuthRules rule-set.
Gateway Action	None
Recommended Action	None.
Revision	1
Context Parameters	User Authentication

2.46.29. challenges_not_supported (ID: 03700108)

Default Severity	NOTICE
-------------------------	--------

Log Message	Challenges are not supported for this authentication system
Explanation	The XAuth authentication system does not support the challenge-and-response method.
Gateway Action	None
Recommended Action	Disable the challenge-and-response feature, and use password verification instead.
Revision	1
Context Parameters	User Authentication

2.46.30. no_shared_ciphers (ID: 03700500)

Default Severity	ERROR
Log Message	SSL Handshake: No shared ciphers exists. Closing down SSL connection
Explanation	No shared ciphers were found between the client and the unit, and the SSL connection can not be established.
Gateway Action	ssl_close
Recommended Action	Make sure that the client and unit share atleast one cipher.
Revision	1
Parameters	client_ip

2.46.31. disallow_clientkeyexchange (ID: 03700501)

Default Severity	ERROR
Log Message	SSL Handshake: Disallow ClientKeyExchange. Closing down SSL connection
Explanation	The Client Key Exchange message received from the client was disallowed, and the SSL connection is closed. This could be a result of SSL handshake message flooding.
Gateway Action	ssl_close
Recommended Action	Investigate the source of this, and try to find out if it is a part of a possible attack, or normal traffic.
Revision	1
Parameters	client_ip

2.46.32. bad_packet_order (ID: 03700502)

Default Severity	ERROR
Log Message	Bad SSL Handshake packet order. Closing down SSL connection

Explanation	Two or more SSL Handshake message were received in the wrong order, and the SSL connection is closed.
Gateway Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.46.33. bad_clienthello_msg (ID: 03700503)

Default Severity	ERROR
Log Message	SSL Handshake: Bad ClientHello message. Closing down SSL connection
Explanation	The ClientHello message (which is the first part of a SSL handshake) is invalid, and the SSL connection is closed.
Gateway Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.46.34. bad_changecipher_msg (ID: 03700504)

Default Severity	ERROR
Log Message	SSL Handshake: Bad ChangeCipher message. Closing down SSL connection
Explanation	The ChangeCipher message (which is a part of a SSL handshake) is invalid, and the SSL connection is closed.
Gateway Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.46.35. bad_clientkeyexchange_msg (ID: 03700505)

Default Severity	ERROR
Log Message	SSL Handshake: Bad ClientKeyExchange message. Closing down SSL connection
Explanation	The ClientKeyExchange message (which is a part of a SSL handshake) is invalid, and the SSL connection is closed.

Gateway Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.46.36. bad_clientfinished_msg (ID: 03700506)

Default Severity	ERROR
Log Message	SSL Handshake: Bad ClientFinished message. Closing down SSL connection
Explanation	The ClientFinished message (which is a part of a SSL handshake) is invalid, and the SSL connection is closed.
Gateway Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.46.37. bad_alert_msg (ID: 03700507)

Default Severity	ERROR
Log Message	Bad Alert message. Closing down SSL connection
Explanation	The Alert message (which can be a part of a SSL handshake) is invalid, and the SSL connection is closed.
Gateway Action	ssl_close
Recommended Action	None.
Revision	1
Parameters	client_ip

2.46.38. unknown_ssl_error (ID: 03700508)

Default Severity	ERROR
Log Message	Unknown SSL error. Closing down SSL connection
Explanation	An unknown error occurred in the SSL connection, and the SSL connection is closed.
Gateway Action	ssl_close
Recommended Action	None.
Revision	1

Parameters client_ip

2.46.39. negotiated_cipher_does_not_permit_the_chosen_certificate_size (ID: 03700509)

Default Severity ERROR

Log Message The negotiated cipher does not permit the chosen certificate size. Closing down SSL connection

Explanation The negotiated cipher was an export cipher, which does not allow the chosen certification size. The certificate can not be sent, and the SSL connection is closed.

Gateway Action ssl_close

Recommended Action Change ciphers and/or certificate.

Revision 1

Parameters client_ip

2.46.40. received_sslalert (ID: 03700510)

Default Severity ERROR

Log Message Received SSL Alert. Closing down SSL connection

Explanation A SSL Alert message was received during an established SSL connection, and the SSL connection will be closed.

Gateway Action close

Recommended Action None.

Revision 1

Parameters client_ip
level
description

2.46.41. sent_sslalert (ID: 03700511)

Default Severity ERROR

Log Message Sent SSL Alert. Closing down SSL connection

Explanation The unit has sent a SSL Alert message to the client, due to some abnormal event. The connection will be closed down.

Gateway Action close

Recommended Action Consult the "description" parameter, which contains the reason for this.

Revision 1

Parameters	client_ip level description
------------	-----------------------------------

2.47. VFS

These log messages refer to the **VFS (VFS file handling events)** category.

2.47.1. odm_execute_action (ID: 05200002)

Default Severity	NOTICE
Log Message	Uploaded file (<filename>) was validated as "<description>". Rebooting system.
Explanation	An uploaded file was validated, and executed. The system will now reboot.
Gateway Action	odm_action_taken
Recommended Action	None.
Revision	1
Parameters	filename description

2.47.2. odm_execute_action (ID: 05200003)

Default Severity	NOTICE
Log Message	Uploaded file (<filename>) was validated as "<description>". Doing system RECONFIGURE .
Explanation	An uploaded file was validated, and executed. The system will now RECONFIGURE.
Gateway Action	odm_action_taken
Recommended Action	None.
Revision	1
Parameters	filename description

2.47.3. odm_no_execute_action (ID: 05200004)

Default Severity	NOTICE
Log Message	Uploaded file (<filename>) could not be recognized as a known type.
Explanation	An uploaded file could not be recognized as a known type.
Gateway Action	odm_no_action_taken
Recommended Action	None.
Revision	1
Parameters	filename

description

2.47.4. pkg_execute_fail (ID: 05200005)

Default Severity	WARNING
Log Message	Uploaded package file (<filename>) could not be executed correctly.
Explanation	An uploaded file was validated but could not be executed correctly. This could be because the unit is out of disk space or that the disk is corrupt.
Gateway Action	None
Recommended Action	Check that the disk is intact and that it has enough space.
Revision	1
Parameters	filename

2.47.5. upload_certificate_fail (ID: 05200006)

Default Severity	NOTICE
Log Message	Certificate data in file <filename>, could not be added to the configuration
Explanation	Certificate data could not be added to the configuration.
Gateway Action	None
Recommended Action	Make sure that the certificate data is of the correct format.
Revision	1
Parameters	filename

2.47.6. upload_certificate_fail (ID: 05200007)

Default Severity	NOTICE
Log Message	Certificate data in file <filename>, could not be added to the configuration
Explanation	Certificate data could not be added to the configuration.
Gateway Action	None
Recommended Action	Make sure that the certificate data is of the correct format.
Revision	1
Parameters	filename

