List of features in the VAST 2012 2nd mini challenge. Features were obtained after data exploration, as part of the modelling of the Normal Operating Conditions (NOC) of the network.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Feature | Source | Description | Sec. Score  (weight) |
| 1 | fw\_asa21 | Firewall Cisco Syslog | Message %ASA-2-106001 | 7 |
| 2 | fw\_asa3 | Firewall Cisco Syslog | Message %ASA-3-\* | 6 |
| 3 | fw\_asa33 | Firewall Cisco Syslog | Message %ASA-3-305006 | 6 |
| 4 | fw\_asa37 | Firewall Cisco Syslog | Message %ASA-3-710003 | 6 |
| 5 | fw\_asa4 | Firewall Cisco Syslog | Message %ASA-4-\* | 5 |
| 6 | fw\_asa41 | Firewall Cisco Syslog | Message %ASA-4-106023 | 5 |
| 7 | fw\_asa44 | Firewall Cisco Syslog | Message %ASA-4-405001 | 5 |
| 8 | fw\_asa5 | Firewall Cisco Syslog | Message %ASA-5-\* | 4 |
| 9 | fw\_asa517 | Firewall Cisco Syslog | Message %ASA-5-111007[[1]](#footnote-1) | 4 |
| 10 | fw\_asa518 | Firewall Cisco Syslog | Message %ASA-5-111008 | 4 |
| 11 | fw\_asa6 | Firewall Cisco Syslog | Message %ASA-6-\* | 3 |
| 12 | fw\_asa610 | Firewall Cisco Syslog | Message %ASA-6-106015 | 3 |
| 13 | fw\_asa611 | Firewall Cisco Syslog | Message %ASA-6-110003 | 3 |
| 14 | fw\_asa630 | Firewall Cisco Syslog | Message %ASA-6-302010 | 3 |
| 15 | fw\_asa6310 | Firewall Cisco Syslog | Message %ASA-6-305010 | 3 |
| 16 | fw\_asa633 | Firewall Cisco Syslog | Message %ASA-6-302013 | 3 |
| 17 | fw\_asa634 | Firewall Cisco Syslog | Message %ASA-6-302014 | 3 |
| 18 | fw\_asa635 | Firewall Cisco Syslog | Message %ASA-6-302015 | 3 |
| 19 | fw\_asa636 | Firewall Cisco Syslog | Message %ASA-6-302016 | 3 |
| 20 | fw\_asa639 | Firewall Cisco Syslog | Message %ASA-6-305009 | 3 |
| 21 | fw\_asa66 | Firewall Cisco Syslog | Message %ASA-6-6050051 | 3 |
| 22 | fw\_asa671 | Firewall Cisco Syslog | Message %ASA-6-7250011 | 3 |
| 23 | fw\_asa672 | Firewall Cisco Syslog | Message %ASA-6-7250021 | 3 |
| 24 | fw\_asa673 | Firewall Cisco Syslog | Message %ASA-6-7250031 | 3 |
| 25 | fw\_asa677 | Firewall Cisco Syslog | Message %ASA-6-7250071 | 3 |
| 26 | fw\_conbuilt | Firewall Cisco Syslog | Connections built | 1 |
| 27 | fw\_condown | Firewall Cisco Syslog | Connections down | 1 |
| 28 | fw\_empty | Firewall Cisco Syslog | Protocol ‘(empty)’ | 2 |
| 29 | fw\_inbound | Firewall Cisco Syslog | Direction: Inbound | 2 |
| 30 | fw\_ipdc | Firewall Cisco Syslog | IP Address Domain Controller | 1 |
| 31 | fw\_ipdns | Firewall Cisco Syslog | IP Address DNS Root Servers | 1 |
| 32 | fw\_ipfwhq | Firewall Cisco Syslog | IP Address Firewall DataCenter | 7 |
| 33 | fw\_ipfwr | Firewall Cisco Syslog | IP Address Firewall Cisco ASA | 7 |
| 34 | fw\_iplog | Firewall Cisco Syslog | IP Address Log Server | 1 |
| 35 | fw\_ipout | Firewall Cisco Syslog | IP Address Others | 1 |
| 36 | fw\_ipservers | Firewall Cisco Syslog | IP Address Financial Servers | 3 |
| 37 | fw\_ipweb | Firewall Cisco Syslog | IP Address Websites | 1 |
| 38 | fw\_ipws | Firewall Cisco Syslog | IP Address Workstations | 1 |
| 39 | fw\_opbuilt | Firewall Cisco Syslog | Operation ‘Built’ | 1 |
| 40 | fw\_opcommand | Firewall Cisco Syslog | Operation ‘Command executed’ | 3 |
| 41 | fw\_opdeny | Firewall Cisco Syslog | Operation ‘Deny’ | 3 |
| 42 | fw\_opdenyacl | Firewall Cisco Syslog | Operation ‘Deny by ACL’ | 3 |
| 43 | fw\_opempty | Firewall Cisco Syslog | Operation ‘(empty)’ | 3 |
| 44 | fw\_opteardown | Firewall Cisco Syslog | Operation ‘Teardown’ | 3 |
| 45 | fw\_outbound | Firewall Cisco Syslog | Direction: Outbound | 1 |
| 46 | fw\_pdce | Firewall Cisco Syslog | Port 135 | 1 |
| 47 | fw\_pdns | Firewall Cisco Syslog | Port 53 | 1 |
| 48 | fw\_pftp | Firewall Cisco Syslog | Port 21 | 3 |
| 49 | fw\_phttp | Firewall Cisco Syslog | Port 80 | 1 |
| 50 | fw\_phttps | Firewall Cisco Syslog | Port 443 | 1 |
| 51 | fw\_pident | Firewall Cisco Syslog | Port 113 | 1 |
| 52 | fw\_pkerberos | Firewall Cisco Syslog | Port 88 | 3 |
| 53 | fw\_pldap | Firewall Cisco Syslog | Port 389 | 3 |
| 54 | fw\_pnetbios1 | Firewall Cisco Syslog | Port 137 | 1 |
| 55 | fw\_pnetbios2 | Firewall Cisco Syslog | Port 138 | 1 |
| 56 | fw\_pnetbios3 | Firewall Cisco Syslog | Port 139 | 1 |
| 57 | fw\_pnstd | Firewall Cisco Syslog | Port > 1024 | 1 |
| 58 | fw\_pshell | Firewall Cisco Syslog | Port 514 | 5 |
| 59 | fw\_psmb | Firewall Cisco Syslog | Port 445 | 1 |
| 60 | fw\_psnmp | Firewall Cisco Syslog | Port 161 | 3 |
| 61 | fw\_pssh | Firewall Cisco Syslog | Port 22 | 5 |
| 62 | fw\_ptelnet | Firewall Cisco Syslog | Port 23 | 5 |
| 63 | fw\_syscritical | Firewall Cisco Syslog | Critical Message | 6 |
| 64 | fw\_syserror | Firewall Cisco Syslog | Error Message | 5 |
| 65 | fw\_sysinfo | Firewall Cisco Syslog | Information Message | 2 |
| 66 | fw\_sysnotice | Firewall Cisco Syslog | Notification Message | 3 |
| 67 | fw\_syswarn | Firewall Cisco Syslog | Warning Message | 4 |
| 68 | fw\_tcp | Firewall Cisco Syslog | Protocol TCP | 1 |
| 69 | fw\_udp | Firewall Cisco Syslog | Protocol UDP | 1 |
| 70 | ids\_badtraffic | IDS Snort | Potentially Bad TRaffic | 7 |
| 71 | ids\_command | IDS Snort | Generic Protocol Command Decode | 3 |
| 72 | ids\_ipdc | IDS Snort | IP Address Domain Controller | 3 |
| 73 | ids\_ipdns | IDS Snort | IP Address DNS Root Servers | 3 |
| 74 | ids\_ipfwhq | IDS Snort | IP Address Firewall DataCenter | 9 |
| 75 | ids\_ipfwr | IDS Snort | IP Address Firewall Cisco ASA | 9 |
| 76 | ids\_iplog | IDS Snort | IP Address Log Server | 3 |
| 77 | ids\_ipout | IDS Snort | IP Address Others | 3 |
| 78 | ids\_ipservers | IDS Snort | IP Address Financial Servers | 5 |
| 79 | ids\_ipweb | IDS Snort | IP Address Websites | 3 |
| 80 | ids\_ipws | IDS Snort | IP Address Workstations | 3 |
| 81 | ids\_ldns | IDS Snort | ET POLICY DNS Update from External net | 3 |
| 82 | ids\_leak | IDS Snort | Attempted Information Leak | 7 |
| 83 | ids\_limap | IDS Snort | ET SCAN Rapid IMAP Connections – Possible Brute Force Attack | 5 |
| 84 | ids\_lirc | IDS Snort | ET POLICY IRC authorization message | 7 |
| 85 | ids\_lnetbios | IDS Snort | GPL NETBIOS | 3 |
| 86 | ids\_lpop3 | IDS Snort | ET SCAN Rapid POP3 Connections – Possible Brute Force Attack | 5 |
| 87 | ids\_lsnmp | IDS Snort | GPL SNMP request tcp | 3 |
| 88 | ids\_lsql | IDS Snort | ET POLICY Suspicious inbound to SQL | 7 |
| 89 | ids\_lssh | IDS Snort | ET SCAN Potential SSH Scan | 7 |
| 90 | ids\_lvnc | IDS Snort | ET SCAN Potential VNC Scan | 7 |
| 91 | ids\_misc | IDS Snort | Misc Activity | 3 |
| 92 | ids\_pdce | IDS Snort | Port 135 | 3 |
| 93 | ids\_pdns | IDS Snort | Port 53 | 3 |
| 94 | ids\_pftp | IDS Snort | Port 21 | 5 |
| 95 | ids\_phttp | IDS Snort | Port 80 | 3 |
| 96 | ids\_phttps | IDS Snort | Port 443 | 3 |
| 97 | ids\_pident | IDS Snort | Port 113 | 3 |
| 98 | ids\_pkerberos | IDS Snort | Port 88 | 5 |
| 99 | ids\_pldap | IDS Snort | Port 389 | 5 |
| 100 | ids\_pnetbios1 | IDS Snort | Port 137 | 3 |
| 101 | ids\_pnetbios2 | IDS Snort | Port 138 | 3 |
| 102 | ids\_pnetbios3 | IDS Snort | Port 139 | 3 |
| 103 | ids\_pnstd | IDS Snort | Port > 1024 | 3 |
| 104 | ids\_prio1 | IDS Snort | Priority 1 | 10 |
| 105 | ids\_prio2 | IDS Snort | Priority 2 | 7 |
| 106 | ids\_prio3 | IDS Snort | Priority 3 | 3 |
| 107 | ids\_privacy | IDS Snort | Potential Corporate Privacy Violation | 10 |
| 108 | ids\_pshell | IDS Snort | Port 514 | 7 |
| 109 | ids\_psmb | IDS Snort | Port 445 | 3 |
| 110 | ids\_psnmp | IDS Snort | Port 161 | 5 |
| 111 | ids\_pssh | IDS Snort | Port 22 | 7 |
| 112 | ids\_ptelnet | IDS Snort | Port 23 | 7 |

Information about syslog ASA format from CISCO can be found here:

<http://www.cisco.com/c/en/us/td/docs/security/asa/syslog-guide/syslogs.html>

1. This is a parsing error. This feature was erroneously introduced in the CSV files, while it is not present in the original logs. [↑](#footnote-ref-1)