WSA S-Series AsyncOS 7.0 Access Logs Format : IronPort Additions

BLOCK_ADMIN_SIZE_11-HR-DefaultGroup-ScanPartnerBoundTraffic-NONE-NONEPartnerProxyPolicy

ACL Decision Tag — AccessOrDecryptionPolicyGroup — IdentityPolicyGroup —OutboundMalwareScanningPolicyGroup — DataSecurityPolicyGroup — ExternalDLPPolicyGroup — RoutingPolicyGroup

ACL decision tag
DEFAULT_CASE - apply Access Policies default
ALLOW_WBRS - Allow due to WBRS of access policy
ALLOE_CUSTOMCAT – Allow due to custom URL category of access policy
REDIRECT_CUSTOMCAT – Redirect due to custom URL category of access policy
BLOCK_[ADMIN | WEBCAT | CUSTOMCAT | WBRS | SUSPECT_USER_AGENT | AMW_REQ | AMW_RESP| AVC] – Block as above
BLOCK_SEARCH_UNSAFE – Client unsafe search matched, action is Block
BLOCK_UNSUPPORTED_SEARCH_APP – Unsupported search engine matched, action is
DECRYPT_ADMIN – Decrypt due to policy default or invalid cert handling
DECRYPT_WEBCAT – decrypt due to predefined URL category
DECRYPT_CUSTOMCAT – decrypt due to custom URL category
DECRYPT_WBRS – decrypt due to WBRS
DROP_[ADMIN | WEBCAT | CUSTOMCAT | WBRS] – drop as above
PASSTHRU_ [ADMIN | WEBCAT | CUSTOMCAT | WBRS] - pass through (tunnel) w/o decryption (only in transparent mode)

The dynamically generated number at the end of the ACL decision tag (**"11"** in this example) is used internally by the Web Proxy to increase performance. You can ignore this number.

Fields inside the angled brackets

URL Category Prefices:
"C_ ": Custom URL category
"IW_ " :Cisco IronPort Web Usage Controls
No prefix: IronPort URL filters .

Field 1-7: URL Filters and Web Reputation Filters. And Webroot information
`<IW_comp,4.7, "Worm","Worm-Licat",100,77915,12524,`
URL Category (nc = no category), WBRS (ns = no score), Webroot Verdict, Spyname, TRR (if one exists), ThreatID, TraceID

Fields 8-13: McAfee
`"Virus","-",0,1,6,"EICAR test file",` ← McAfee Verdict, File name, Scan Error Code, Detection Type, Virus Type, Virus Name

Fields 14-17: Sophos
`Encrypted File","-2147220974","Confidential.zip","-",` ← Sophos Verdict, Scan Return Code, File Locations, Threat Name

Fields 18-19: Data Security and Data Loss Prevention
`0,1,` ← IronPort Data Security Verdict, External DLP Server Verdict (0 = Allow, 1 = Block, hyphen = Unscanned),

Fields 20-23: URL Category Verdicts, Unified inbound DVS verdict, Web Reputation Filter Threat Type
`IW_comp,-, "Adware","phishing",`
Request-side URL verdict, Response-side URL verdict, Unified Inbound DVS Verdict, Web Reputation Filter Threat Type

URL verdicts: "`IW_xxxx,-`" means DCA not used
"`nc,IW_xxxx`" means DCA classified URL

Fields 24-25: Application Visibility and Control
`"WebEx","Presentation/Conferencing","Unknown","-",`
Application Name, Application Type, Application Behavior, Safe Browsing Scanning Verdict,

Fields 26-28: Bandwidth & Type of User
`16789.33,0,-`
Average Bandwidth (Kb/sec), Throttle Flag, Type of User

Trottle Flag: "`0`" means bandwidth was not throttled
"`1`" means DCA engine classified URL
Type of User: "`Local`" – Mobile Use Security classifies user as local
"`Remote`" – Mobile Use Security classifies user as remote
"-"(hypen) – Mobile Use Security is disabled

Fields 29-30: Outbound Malware Scanning
`"Virus","Mal/DownLdr-AC">` ← Unified Outbound DVS Verdict, Outbound Threat Name

WSA S-Series AsyncOS 7.0 Access Logs Format: squid default

```
1215535247.487 123 172.20.11.222 TCP_MISS/200 14148 GET http://www.cisco.com/ "Hegel Hotel@Hotel"
```

%t - time stamp in unix time

%e - elapsed time

%a - client IP address

%w – Transaction result code

%h - HTTP response code

%s - total bytes

%r - requestmethod URI

%A - authenticated user

```
DIRECT/www.cisco.com text/html
```

%H – cache hierarchy retrieval
NONE no request made
DIRECT request went directly to server
DEFAULT_PARENT – single upstream proxy or failover
LEASTBUSY_PARENT – Fewest connections
HASHBASED_PARENT– Hash based load balancing
LEASTRECENT_PARENT– Least recently used
ROUNDROBIN_PARENT– Round robin load balancing

%d - data source (domain)

%c – MIME content type/subtype

NONE - Neither a hit nor a miss, indicates an error in the transaction
TCP_HIT - Object was cached in the disk
TCP_MEM_HIT - Object was cached in memory
TCP_IMS_HIT - Client sends an 'If-Modified-Since' request to the proxy and proxy responds with '304 Not modified'.
TCP_REFRESH_HIT - Client sends a normal request, cached object has expired, proxy sends an 'If-Modified-Since' request to server, server responds with '304 Not Modified', proxy responds back with '200 Ok' response but sets flag as TCP_REFRESH_HIT.
TCP_REFRESH_HIT_SSL – HTTPS refresh hit as above
TCP_MISS - Object was not present in the cache
TCP_MISS_SSL – HTTPS Object was not present in the cache
TCP_CLIENT_REFRESH_MISS - Client request explicitly contained headers to not serve cached content
TCP_CLIENT_REFRESH_MISS_SSL – HTTPS refresh miss
TCP_DENIED – Access denied
TCP_DENIED_SSL – HTTPS Access denied

Some HTTP response codes

200 OK
204 No content
206 Partial content
301 Moved Permanently
302 Found (over there)
304 Not modified
305 Use Proxy
307 Temporary Redirect
401 Unauthorized
403 Forbidden
404 Not Found
405 Method not allowed
407 Proxy Auth required
503 Service Unavailable
504 Gateway timeout

The log format specifiers **(Bold font fields are logged by default)**

%a - client IP address
%A - authenticated user
%b - body bytes returned
%B - total bytes used (%b+%q)
%c - content type
%C - cookie header
%d - data source (domain)
%D - ACL decision tag
%e - elapsed time
%E - error type
%f - X-Forwarded-For header
%F - client source port
%g - authorized group names
%h - HTTP response code
%H - cache hierarchy retrieval
%i – IP address of ICAP server
%I - transaction ID
%j - don't cache response (DCF) flags
%k - Data Source IP address
%l - Type of User for Mobile User Security (Local or Remote)
%L - request local time [DD/MMM/YYYY:hh:mm:ss +nnnn]
%m - authentication mechanism (BASIC, NTLMSSP, SSO_ASA, etc.)
%M - cache miss flags
%N - Server Name or Dest. Host Name
%p - Destination Port Number
%P - Protocol
%q - Request size (headers + body)
%r - req. first line: request method, URI, HTTP version
%R - referer
%s - total bytes
%t - UNIX epoch time stamp
%T - timeout code
%u - user agent
%U - request URI
%v - request local date [YYYY-MM-DD]
%V - request local time [hh:mm:ss]
%w - result code (TCP_MISS, TCP_REFRESH_HIT, etc...)
%W - result code with denial cause
%x - latency
%Xa - URL Category response numeric code
%XA - URL Category response abbr.
%Xb - Web Application behavior (AVC)
%XB - average bandwidth (Kb/sec)
%Xc - URL Category numeric code
%XC - URL Category abbreviation
%Xd - McAfee scan verdict
%Xe - McAfee file name
%Xf - McAfee scan error code
%XF - Full name of custom URL category
%Xg - McAfee detect type
%XG - AVC request header verdict
%Xh - McAfee virus type
%XH - AVC request body verdict
%Xi - Webroot TraceID
%Xj - McAfee virus name
%Xk - Web Rep. threat type
%XK - Web Rep. threat reason
%Xl - IDS scanning verdict
%XL - URL Category response full name
%XM - AVC response header verdict
%Xn - Threat name (Spyname)
%XN - AVC response body verdict
%XO - Web Application (AVC)
%Xp - external DLP scanning verdict
%Xq - URL Category request numeric code
%XQ - URL Category request abbr.
%Xr - <Web Rep & MW> 6 fields
%XR - URL Cate. request full name
%Xs - Webroot spyID
%XS - Safe browsing \verdict
%Xt - Webroot TRR
%XT - bandwidth throttle flag
%Xu - Web Application Type (AVC)
%Xv - Webroot scan verdict
%Xw- Raw numeric WBRS score
%XW - Decoded WBRS score
%Xx - Sophos scan return code
%Xy - Sophos threat location
%Xz - Sophos threat name
%XZ - Resp. DVS verdict name
%X0 - DVS: resp. verdict
%X1 - DVS resp. threat name
%X2 - DVS req. verdict
%X3 - DVS req. verdict name
%X4 - DVS req. threat name
%y - method (GET, POST, etc.)
%Y - entire URL
%<*Request_header_to_include*
%>*Response_header_to_include*
%: - Event Time
%$ - Logging Format ID