totalsecurity™

Check Point SOFTWARE TECHNOLOGIES LTD.

LEA Fields Update

Partner Solutions
June 2014
Draft

Introduction

This document is an update to fields listed in the LEA (Log Export API) specification which enables a third party application to securely receive both real-time and historical auditing log data generated by Check Point devices.

Notes:

- This is not a full list of the log fields that a Check Point device will generate.
- When known the LEA field data type and whether or not there is a dictionary available is noted.
- See the product release for product name changes.
- For additional information on field descriptions see the SmartView Tracker section of the Security Management Administration Guide. The Tracker names are translated values and may not be the same as the raw field name available via LEA.

Common Fields

Listed below are some log fields common to most applications in alphabetical order. If a field is not used it will not be in the LEA lookup dictionary.

Notes:

- Some of the field names end with a ":" character. For example, "reason" and "reason:" are two different fields.
- Beginning in NG AI R54 two fields were introduced to capture successive log events. These are the "Total logs" and "Successive logs" fields. When providing counts of events these field values can be checked.

Field	Data Type	Description/Values	Dictionary
action	LEA_VT_ACTION	The action taken in enforcing the security policy (ctl, accept, reject, drop, encrypt, decrypt, authcrypt, authorize, deauthorize)	Yes
alert	LEA_VT_ALERT	the type of alert. The presence of this field is the only reliable indication that the log entry is an alert type entry. Values = "alert, snmptrap, mail, useralert, useralert2, useralert3"	Yes
d_port	LEA_VT_UDP_PORT or LEA_VT_TCP_PORT or LEA_VT_USHORT	the destination port number	Yes
dst	LEA_VT_IP_ADDR	the IP address of the connection destination	Yes
i/f_dir	LEA_VT_DIRECTION	The direction of the connection with respect to	Yes

		the interface (e.g. “inbound”, “outbound”).	
i/f_name	LEA_VT_INTERFACE	The interface through which this connection passed, “daemon” if generated internally (e.g. “le0”, “E190x2”).	Yes
icmp-code	LEA_VT_INT	ICMP code	No
icmp-type	LEA_VT_INT	ICMP type	No
message_info	LEA_VT_STRING	Informational message – stating why the packet was dropped	No
orig	LEA_VT_IP_ADDR	IP address of the device that generated the log entry	Yes
product	LEA_VT_STRING	Check Point or OPSEC partner product name(s)	No
proto	LEA_VT_IP_PROTO	the ip protocol	No
reason	LEA_VT_STRING	For alerts, a description of why the alert was generated (e.g. “unknown user”).	No
reason:	LEA_VT_STRING	Messages sent by the VPN-1/FireWall-1 kernel.	No
rule	LEA_VT_RULE	if greater than zero, the number of the Security Policy rule applied to the connection. Otherwise, a dictionary is specified, and the rule’s value can be converted into string (e.g. “internal”).	if < 0
s_port	LEA_VT_UDP_PORT or LEA_VT_TCP_PORT or LEA_VT_USHORT	the source port number	Yes
service	LEA_VT_UDP_PORT or LEA_VT_TCP_PORT or LEA_VT_STRING or LEA_VT_USHORT	the destination port number for well known services	Yes
src	LEA_VT_IP_ADDR	the IP address of the connection source	Yes
sys_msgs/sys_message	LEA_VT_STRING	The reason for the control log (e.g. “started sending log to localhost”).	Yes
time	LEA_VT_TIME	the date and time the log entry was written	No
uuid	LEA_VT_UUID	the uuid of the log chain	No
xlatedport	LEA_VT_UDP_PORT or LEA_VT_TCP_PORT	The translated destination port (when NAT is performed)	Yes
xlatedst	LEA_VT_IP_ADDR	The translated IP address of the source (when NAT is performed)	Yes
xlatesport	LEA_VT_UDP_PORT or LEA_VT_TCP_PORT	The translated source port (when NAT is performed)	Yes
xlatesrc	LEA_VT_IP_ADDR	the translated IP address of the source (when NAT is performed).	Yes

Accounting

When a user specifies Account as the Track option, in a Security Policy rule for instance, byte information is included in the log record.

Note: Log records are composed of fragments and fragments of the same chain might be spread over the log file and sometimes even across file boundaries. When the file read mode is Unified updates in the form of record fragments like accounting bytes are not available in LEA_ONLINE mode. When the file read mode is not Unified then record fragment updates should not be counted as separate connections.

Field	Data Type	Description/Values	Dictionary
bytes	LEA_VT_INT	The number of bytes transmitted in the connection.	No
elapsed	LEA_VT_DURATION_TIME	the duration of the connection	No
has_accounting	LEA_VT_INT	When 1, this indicates that the log record has a matching record in the accounting log	No
packets	LEA_VT_INT	The number of packets in the session	No
segment_time	LEA_VT_TIME	Presence of this field indicates the connection has closed.	No
start_time	LEA_VT_TIME	The date and time the connection started. Use the elapsed field to calculate the time the connection ended.	No

Content Security, Security Servers, and Legacy Authentication

Content security requires inspection of Application layer traffic. Security Servers are legacy Check Point processes that that perform Content Security for HTTP, FTP, and SMTP. Security Servers employ many ways of enforcing content security including, for example checking whether the connections for these protocols are well formed, stripping script tags for HTTP, email address translation for SMTP and file name matching for FTP.

In addition to Content Security, Security Servers perform legacy User Authentication for telnet and rlogin. Client Authentication and Session Authentication are additional legacy authentication methods.

Field	Data Type	Description	Dictionary
agent	LEA_VT_STRING	The SMTP security server agent,	

		e.g. ”mail server” or ”mail dequeuer”	
auth_method:		When client authentication is used the auth method e.g. “Std Sign On”.	
cat_server	LEA_VT_STRING	The name of the UFP server (HTTP).	No
category	LEA_VT_MASK	UFP mask (e.g. “drugs”, “alcohol”). Use lea_resolve_field to resolve all relevant categories. Use lea_dictionary_lookup to resolve only one category. (HTTP)	Yes
from	LEA_VT_STRING	The translated email address of the sender (SMTP).	No
orig_from	LEA_VT_STRING	Address of the original sender (SMTP).	No
orig_to	LEA_VT_STRING	Address of the original recipient (SMTP).	No
reason	LEA_VT_STRING	Authentication method including, e.g. “Non-auth login: anonymous”, “Authenticated by FireWall-1 Password”, and “Access denied – wrong username or password”.	No
reason:	LEA_VT_STRING	An authentication message, e.g. “Client Encryption: Authenticated by Internal Password”.	No
reject_category		Reason for an authentication failure. Examples include “Authentication Failure|IKE failure|Gateway to Gateway authentication failure|SecureClient authentication failure”	
res_action	LEA_VT_STRING	The direction of an FTP file copy operation (e.g. “get”, “put”) (FTP).	No
resource	LEA_VT_STRING	The URL accessed (e.g. http://a.b.c.d:80/ or ftp://a.b.c.d/pub/readme.txt) (FTP & HTTP). When the HTTP resource method is Optimize URL logging, then the URL will be of the form “http://www.name.com/” or “http://a.b.c.d/”.	No

Service_name		Protocol type that matches the security server (e.g. “ftp”, “http”, “telnet”).	
srcname	LEA_VT_STRING	The name of the Session Auth agent host.	Yes
to	LEA_VT_STRING	The translated email address of the original recipient (SMTP).	No
user	LEA_VT_STRING	The user name. The value may be “<no_auth> if the resource rule does not require authentication.	No

Identity Awareness

Introduced in R71 as Identity Logging this provides granular visibility and control of users, groups and machines. Identity aware gateways get identities from one or a combination of these identity sources; AD Query, Captive Portal, Light Identity Agent and can be configured to share this information with other identity aware gateways.

Field	Data Type	Description/Values	Dictionary
product		Identity Logging or Identity Awareness or VPN1 & FireWall-1	
dst_machine_name		Resolved AD name of a machine associated with destination IP of a logged traffic	
dst_user_name		Resolved AD name of a user associated with destination IP of a logged traffic	
src_machine_name		Resolved AD name of a machine associated with source IP of a logged traffic	
src_user_name		Resolved AD name of a user associated with source IP of a logged traffic	
domain_name			
termination_reason			
duration			
identity_type			
description		for example ―Session Expiration‖	
endpoint_ip			
identity_src		for example AD Query	
information			
snid			

Encryption

IPsec VPN creates encrypted tunnels with other gateways and remote clients by using the Internet Key Exchange (IKE) and IP Security (IPSec) protocols.

Field	Data Type	Description/Values	Dictionary
community	LEA_VT_STRING	A collection of VPN gateways	
CookieI	LEA_VT_STRING	The ID of the negotiation — sent for ISAKMP Phase One	No
CookieR	LEA_VT_STRING	The ID of the negotiation — sent for ISAKMP Phase Two	No
decryption failure:	LEA_VT_STRING	A string describing why the encryption failed	No
dstkeyid	LEA_VT_STRING	The destination's encryption key ID. For ISAKMP this is the destination SPI.	No
encryption failure:	LEA_VT_STRING	A string describing why the encryption failed	No
encryption fail reason		A string describing why the encryption failed	
IKE IDs:		The peer's identity, e.g. "subnet: 0.0.0.0 (mask= 0.0.0.0) and host: a.b.c.d".	
IKE log:	LEA_VT_STRING	Messages and error text	No
IKE:		The IKE negotiation phase, e.g. "Main Mode completion".	
methods:	LEA_VT_STRING	A string consisting of three tokens separated by commas, as follows: • encryption method used to generate the session key • encryption algorithm for the session • hashing algorithm for the session	No
peer gateway	LEA_VT_IP_ADDR	the peer gateway	
scheme:	LEA_VT_STRING	The encryption scheme used, e.g. "IKE" or "SSL".	No
srckeyid	LEA_VT_STRING	The source's encryption key ID. For ISAKMP this is the source SPI.	No
success reason:	LEA_VT_STRING	A string describing why the decryption succeeded (e.g. "gateway connected to both end points").	No

Internal CA (Certificate Authority)

The ICA is a Certificate Authority which is an integral part of the Check Point Security Management. It is fully compliant with X.509 standards for both certificates and CRLs.

Field	Data Type	Description	Dictionary
dn:		An object SIC name.	
DN:		DN of the peer object.	
Instruction:		Instructions to the operator, e.g. "If this log persists, contact the CA administrator."	
Internal_CA:		Messages coming from the Internal CA to be logged, e.g. "Issued a new CRL <x>".	
Reason:		The reason for the error, e.g. "No valid CRL".	
serial_num:		Serial number of the certificate	
Validation log:		Result of the validation operation, e.g. "Certificate <name> cannot be validated."	

VPN Client Related

Remote access clients include SecuRemote, SecureClient, Endpoint Connect, and SSL Network Extender. Office Mode enables a VPN gateway to assign a remote client an IP address. The assignment takes place once the user connects and authenticates.

Endpoint Security on Demand (ESOD). When end users access the User Portal for the first time, they are prompted to download an ActiveX component that scans the end user machine for malware and other security related settings. In Security Gateway R70 the product name changed from ICS to ESOD, Endpoint Security On Demand. See the Connectra section for a list of ESOD fields.

Note: The user name and authentication method is also available. See the section Content Security, Security Servers, and Authentication.

Field	Data Type	Description/Values	Dictionary
assigned_IP:		The IP address assigned via office mode.	
OM:		Assigned IP address for <x> seconds".	
om_method:		The IP pool method, e.g. "manual list" or "dhcp".	

SecureClient and Endpoint Security VPN

SecureClient and Endpoint Security VPN are remote VPN clients that extend security to the desktop by allowing your security administrators to define and enforce desktop security policies of mobile users. Logs from rules in the desktop policy where the Track option is Alert will be uploaded to the Policy server and be accessible to LEA clients. The logs contain some common fields like time, action, orig, i/f_dir, i/f_name, alert, product, src, s_port, dst, service, proto, rule, and user.

Field	Data Type	Description/Values	Dictionary
orig	LEA_VT_IP_ADDR	The IP address of the SecureClient host.	Yes
product	LEA_VT_STRING	The value will be “SecureClient”.	No
site_name		The VPN-1 gateway that the client is connecting to.	
user	LEA_VT_STRING	The value will be “default” when the client is not connected to a Policy Server and will be the valid user when connected.	No

SSL VPN – Mobile Access Software Blade

The Mobile Access Software Blade introduced in the R75 release is integrated SSL VPN with integrated Web Intelligence to inspect Web traffic and endpoint security to defend against insecure endpoints.
Connectra includes Endpoint Security on Demand (ESOD). When end users access the User Portal for the first time, they may be prompted to download an ActiveX component that scans the end user machine for malware and other security related settings. The SSL VPN technology was formerly known as the dedicated SSL VPN product Connectra. Events from the Mobile Access Blade still have the product name Connectra.

Field name	Data Type	Description	Dictionary
access_status	LEA_VT_STRING	Example: ”Allowed”, ”Denied”	
Anti_Virus_type	LEA_VT_STRING	Example: ”Not installed”	
auth_method	LEA_VT_STRING	Internal Password, Radius, etc.	
auth_status	LEA_VT_STRING	Example: ”Failure”, ”Logout”, ”Resumed”, ”Success”, ”Timeout”	
Client Type		Example: ”Endpoint WINDOWS”	
cvpn_category	LEA_VT_STRING	Example: ”Client Security”, ”File Shares”, ”Native Mail”, ”Portal”, ”Session”, ”Web”, ”Web Intelligence”, Web Mail”	
cvpn_resource	LEA_VT_STRING	the name of the Application from the	

		Connectra Administrator User Interface	
description	LEA_VT_STRING	Example: ”Request allowed access”, ”Request denied”	
dst	LEA_VT_IP_ADDR	IP address of the destination	Yes
dstname		Example: ” clients1.google.com”	
End_User_Firewall_type	LEA_VT_STRING	Example: ”Not authorized – status not installed”	
ESOD_Associated_Policies		Example: ” This rule is member in policies: 'High security policy'(#1), 'Medium security policy'(#2)”	
ESOD_Noncompliance_Reason		Example: ” zaavkav: Not enabled.”	
ESOD_Rule_Action		Example: ”Restrict”, ”AskUser”	
ESOD_Rule_Name		Example: ” High security Anti-Virus applications check(1)”	
ESOD_Rule_Type		Example: ”Anti Virus”	
fs_dest	LEA_VT_STRING	host share path	
fs_proto	LEA_VT_STRING	Examples: NFS / SMB / CIFS	
group	LEA_VT_STRING	the group the user belongs to	
ICS_access_status **or** ESOD_access_status	LEA_VT_STRING	Example: ”Access Allowed” or ”Access Denied”	
ICS_scan_id	LEA_VT_STRING	A uuid identifying the scan	
ICS_scan_status **or** ESOD_scan_status	LEA_VT_STRING	Example: ”Scan Succeeded” or ”Scan Failed”	
outgoing_url	LEA_VT_STRING	the URL that is visible to the user in the portal	
product	LEA_VT_STRING	product name ”Connectra”	No
reason	LEA_VT_STRING	passed by the Auth module. “failed because”,. etc.	
reject_id	LEA_VT_STRING	for support reason, error number	
request_info	LEA_VT_STRING	Example: “The server is down"	
resource		The URL accessed, Example: ” http://clients1.google.com:80/generate_204”	

s_port	LEA_VT_UDP_PORT or LEA_VT_TCP_PORT or LEA_VT_USHORT	the source port	Yes
service	LEA_VT_UDP_PORT or LEA_VT_TCP_PORT or LEA_VT_STRING or LEA_VT_USHORT	the destination port	Yes
session_duration_time		The duration in minutes of the user's session, Example: "15 minutes"	
snid	LEA_VT_STRING	type is string	
spyware_name	LEA_VT_STRING	Example: "Hitbox"	
spyware_type	LEA_VT_STRING	Example: "3rd Party Cookie"	
src	LEA_VT_IP_ADDR	IP address of the source	Yes
url	LEA_VT_STRING	the url user typed in browser	No
url	LEA_VT_STRING	for web browsing - URL sent by Connectra	
user	LEA_VT_STRING	user	
user_ics **or** user_ESOD		ICS Scan	
user_isb		ISB	
user_proto	LEA_VT_STRING	Web Dav / HTTP	

Integrated IPS

The early IPS product was named SmartDefense. In the Security Gateway R70 release in 2009 the SmartDefense engine was replaced with a new IPS engine and some additional fields were added, but the product field value of SmartDefense was kept in the IPS log events. The best method to keep up to date with the latest changes is to subscribe to IPS News. In each update there is an example log field value.

Note: In general you can key on the product field where the name is SmartDefense. There are other logs that relate to SmartDefense, but historically they have not had the product name of SmartDefense. These logs will be changed in later versions of the product to also include the product value of SmartDefense.

In NG with AI R55, a specific protection type's event is logged with unused rule numbers. For Check Point InterSpect and NG with AI R55W, logged events are descriptive. A full list is available in SecureKnowledge solution sk26226.

When packet captures is enabled on a protection, then the event includes a capture_uuid field. This can be provided to the fwm getpcap to retrieve the packet capture. See the latest CLI reference guide for usage.

Example
loc=96 filename=fw.log fileid=1402093147 time= 6Jun2014 15:19:56 action=drop orig=r77 i/f_dir=inbound i/f_name=eth0 has_accounting=0 product=SmartDefense Protection Name=Non Compliant DNS Severity=4 Confidence Level=3 protection_id=DnsProtocolEnforcement SmartDefense Profile=Recommended_Protection Performance Impact=2 Protection Type=anomaly_dns rule=2 rule_uid={AE831485-A9C8-4681-BE8F-0E2E66904BD} Packet info=query domain length is 64. Attack Info=Bad domain format, query domain exceeding 63 bytes attack=Non Compliant DNS src=192.168.115.181 s_port=32768 dst=192.168.35.181 service=domain-udp proto=udp __policy_id_tag=product=VPN-1 & FireWall-1[db_tag={248E14F5-9CEE-184F-B892-E591BB767615};mgmt=r77;date=1401485698;policy_name=Standard] origin_sic_name=cn=cp_mgmt,o=r77..pcfxuu

Field	Data Type	Description	Dictionary
action	LEA_VT_ACTION	a new action field value ”monitor” may be used instead of ”drop” for instance	Yes
attack	LEA_VT_STRING	attack name	No
Attack Info	LEA_VT_STRING	additional info about the attack	No
message_info	LEA_VT_STRING	In the past and in some cases in current versions, e.g. anti-spoofing and ICMP errors messages, this field is used instead of the above to state why the packet was dropped	No
Packet info	LEA_VT_STRING	additional details about the packet	No
product		most logs will have the value ”SmartDefense”	
capture_uuid		IPS packet capture uuid	
Confidence Level		IPS protection confidence level setting	
Protection Name		IPS protection name	
Severity		IPS protection severity level setting	
protection_id		IPS protection ID	
Duration			
FollowUp		IPS protection Follow-up setting	
Industry Reference		IPS protection industry reference	
Performance Impact		IPS protection performance impact setting	
Protected Server			
Protection Type		IPS protection type	

Antivirus

Antivirus secures content like emails from viruses. The product field value is ”Anti Virus” or “New Anti Virus” which is available in R75.40 and later.

Example
loc=1118 filename=fw.log fileid=1402093147 time= 6Jun2014 15:30:51 action=block orig=r77 i/f_dir=outbound i/f_name=eth2 has_accounting=0 product=New Anti Virus web_client_type=Chrome resource=http://172.25.1.52/mal/eicar.com src=Winsvr2012 s_port=49263 dst=172.25.1.52 service=http proto=tcp session_id=<5392411b,00000002,b17361d1,c0000001> ticket_id={5392411B-1-C0A823AF-C0000001} file name=eicar.com scan result=Infected Protection name=EICAR-Test-File file_type=Command file_md5=44d88612fea8a8f36de82e1278abb02f Protection Type=protection Confidence Level=5 severity=2 log_id=9999 protection_id=0407D7DC6 malware_rule_id={27CC0EC6-7CBE-F54E-AFE0-F46162CEB057} malware_action=Malicious file/exploit download proxy_src_ip=Winsvr2012 scope=Winsvr2012 __policy_id_tag=product=VPN-1 & FireWall-1[db_tag={248E14F5-9CEE-184F-B892-E591BB767615};mgmt=r77;date=1401485698;policy_name=Standard] origin_sic_name=cn=cp_mgmt,o=r77..pcfxuu Suppressed logs=1 sent_bytes=0 received_bytes=0 packet_capture_unique_id=192.168.35.175_maildir_sent_new_time1402093851.mail-3952490649-2213759938.localhost packet_capture_time=1402093851 packet_capture_name=src-192.168.35.175.eml UserCheck_incident_uid=C43F4B24-537D-10B6-9FA9-8A75CAC6B0CD UserCheck=1 portal_message= The site you are trying to access is classified as malicious and has been blocked. For more information, please contact your help desk. Click here to report an incorrect classification. Activity: Malicious file/exploit download URL: http://172.25.1.52/mal/eicar.com Reference: CAC6B0CD UserCheck_Confirmation_Level=Application frequency=1 days

Field Name	Data Type	Description	Dictionary
activity	LEA_VT_STRING	For instance ”Anti Virus Signature Update for SmartCenter”	
data origin	LEA_VT_STRING	The URL of the connection	
email_control		Control	
email_control_analysis		Control analysis	
email_id		Email ID	
email_recipients_num		Recipients number	
email_session_		Email session ID	

id			
file name		The scanned file name, for instance ”eicar.zip”	
file_type		The file type, for instance ”ZIP archive data”	
from		Sender	
product	LEA_VT_STRING	The product field value is “Anti Virus” or “New Anti Virus”.	
scan direction		The direction of the scanned file, for instance from ”Internal to External”	
scan result		The scan result, for instance ”Infected”	
sig_ver		The anti-virus signature version	
subs_exp		The expiration date of the subscription, for instance ”04-Apr-2006”	
to		Recipients	
Update Status		The status of the signature update, for instance ”failed” or ”up-to-date”	
update_src		The update source, for instance ”Remote” or ”SmartCenter”	
virus name	LEA_VT_STRING	The name of the virus found	

Anti-Bot

Check Point Anti-Bot Software Blade
The Check Point Anti-Bot Software Blade detects bot-infected machines, prevents bot damages by blocking bot C&C communications.

Example
loc=4220 filename=fw.log fileid=1402093147 time= 6Jun2014 16:01:57 action=block orig=r77 i/f_dir=outbound i/f_name=eth1 has_accounting=0 product=Anti Malware web_client_type=Chrome resource=http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html src=Winsvr2012 s_port=49600 dst=23.203.225.174 service=http proto=tcp session_id=<53924865,00000002,b17361d1,c0000001> Protection name=Check Point - Testing Bot malware_family=Check Point Confidence Level=5 severity=2 malware_action=Communication with C&C site rule_uid={AE831485-A9C8-4681-BE8F-0E2E66904BDB} Protection Type=URL reputation malware_rule_id={27CC0EC6-7CBE-F54E-AFE0-F46162CEB057} protection_id=00233CFEE refid=0 log_id=9999 proxy_src_ip=Winsvr2012 scope=Winsvr2012 __policy_id_tag=product=VPN-1 & FireWall-1[db_tag={8119E2B3-79E5-4747-80E6-6756E42EE86D};mgmt=r77;date=1402094422;policy_name=Standard] origin_sic_name=cn=cp_mgmt,o=r77..pcfxuu Suppressed logs=1 sent_bytes=0 received_bytes=0

packet_capture_unique_id=192.168.35.175_maildir_sent_new_time1402095718.mail-4230074710-508316721.localhost packet_capture_time=1402095718 packet_capture_name=src-192.168.35.175.eml UserCheck_incident_uid=80E6C145-7AB6-D2C5-1DC5-A500F1473A70 UserCheck=1 portal_message= Your computer is trying to access a malicious server. It is probably infected by malware. For more information and remediation, please contact your help desk. Click here to report an incorrect classification. Activity: Communication with C&C site URL: http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html Reference: F1473A70 UserCheck_Confirmation_Level=Application frequency=1 days

Field Name	Data Type	Description	Dictionary
web_client_type			
resource			
Protection name			
malware_family			
Protection name			
Protection Type			
malware_family			
Confidence Level			
severity			
malware_action			
scope			

Threat Emulation

Check Point ThreatCloud Emulation Service prevents infections from undiscovered exploits, zero-day and targeted attacks. Files are inspected and run in a virtual sandbox to discover malicious behavior.

Example
loc=6236 filename=fw.log fileid=1402093147 time= 6Jun2014 16:24:24 action=prevent orig=r77 i/f_dir=inbound i/f_name=eth2 has_accounting=0 product=Threat Emulation web_client_type=Chrome resource=http://172.25.1.52/mal/MALWARE.pdf src=Winsvr2012 s_port=49791 dst=172.25.1.52 service=http proto=tcp session_id=<00000020,004c0043,b7684fdc,dbed1302> log_id=4000 proxy_src_ip=Winsvr2012 __policy_id_tag=product=VPN-1 & FireWall-1[db_tag={8119E2B3-79E5-4747-80E6-6756E42EE86D};mgmt=r77;date=1402094422;policy_name=Standard] origin_sic_name=cn=cp_mgmt,o=r77..pcfxuu malware_rule_id={27CC0EC6-7CBE-F54E-AFE0-F46162CEB057} scope=Winsvr2012 file_name=MALWARE.pdf file_type=pdf file_size=91010 file_md5=57f8bc2995ca99e20b356b623fa12f29 file_sha1=6e17160f925ac3e376b8f17526629aef71086c16 verdict=Malicious analyzed_on=Check Point Threat Cloud detected_on=Win7,Office 2003/7,Adobe 9

WinXP,Office 2003/7,Adobe 9 TE_verdict_determined_by=Win7,Office 2003/7,Adobe 9: local cache. WinXP,Office 2003/7,Adobe 9: local cache. Protection Name=Exploited pdf document Protection Type=HTTPEmulation severity=4 malware_action=Behaves like a known malware (Exploit.SWF.CVE-2011-0611.bf)
Malicious Filesystem Activity
Malicious Network Activity
Malicious Registry Activity
Unexpected Process Creation
Unexpected Process Termination Confidence Level=5 packet_capture_unique_id={00000020-004C-0043-B768-4FDCDBED1302}7e6fe36e-889e-4c25-8704-56378f0830df {00000020-004C-0043-B768-4FDCDBED1302}e50e99f3-5963-4573-af9e-e3f4750b55e2 {00000020-004C-0043-B768-4FDCDBED1302}00000000-0000-0000-0000-000000000000

Field Name	Data Type	Description	Dictionary
web_client_type			
resource			
scope			
file_name			
type			
file_size			
file_md5			
file_sha1			
verdict			
analyzed_on			
detected_on			
TE_verdict_determined_by			
Protection Name			
Protection Type			
severity			
malware_action			
Confidence Level			

AntiSpam

Anti-Spam and Email Security protect an organization's messaging infrastructure. A multidimensional approach protects the email infrastructure, provides highly accurate spam protection, and defends organizations from a wide variety of virus and malware threats delivered within email. The product field value is ”Anti Spam”. It can be managed from a SmartCenter server.

Field Name	Data Type	Description	Dictionary
email_control		Control	
email_control_analysis		Control analysis	
email_id		Email ID	
email_recipients_num		Recipients number	
email_session_id		Email session ID	
email_spam_category		Spam category	
from		Sender	
scan_direction		File direction	
src_country		Source country	
to		Recipients	

URL Filtering

URL Filtering protects users and enterprises by restricting access to an array of potentially dangerous sites and content, blocking inappropriate Web surfing. The product field value is ”Web Filtering”.

Example
loc=2622 filename=fw.log fileid=1402093147 time= 6Jun2014 15:45:18 action=inform orig=r77 i/f_dir=outbound i/f_name=eth0 has_accounting=0 product=URL Filtering src=Winsvr2012 s_port=49420 dst=23.61.194.224 service=http proto=tcp appi_name=budweiser.com app_id=-1003707612 matched_category=Alcohol app_properties=Alcohol,URL Filtering app_risk=0 app_rule_id={608DB36A-30B6-4321-8416-6832A88130A9} app_rule_name=Block Child Abuse sites web_client_type=Chrome web_server_type=Apache UserCheck_incident_uid=F2D713DB-058F-82AE-51FB-AB0619CAF7A9 resource=http://www.budweiser.com/default.aspx proxy_src_ip=Winsvr2012 __policy_id_tag=product=VPN-1 & FireWall-1[db_tag={8119E2B3-79E5-4747-80E6-6756E42EE86D};mgmt=r77;date=1402094422;policy_name=Standard] origin_sic_name=cn=cp_mgmt,o=r77..pcfxuu UserCheck=1 log_id=9999 user_status=Pending portal_message=Please be reminded that according to the company policy, access to budweiser.com is intended for work-related use only. Reference: 19CAF7A9 UserCheck_Confirmation_Level=Application frequency=1 days

Field Name	Data Type	Description	Dictionary
activity		Activity	

categories		Categories	
reason		Reason	
resource		Resource	
ticket_id		Ticket ID	
uf_sig_ver		URL list version	
matched_category			
appi_name			
app_id			
app_properties			
app_risk			
app_rule_name			
web_client_type			
web_server_type			

Application Control

The Check Point Application Control Software Blade enables IT teams to easily create granular policies to identify, block or limit usage of over 5,000 Web 2.0 applications.

Example
loc=2230 filename=fw.log fileid=1402093147 time= 6Jun2014 15:40:18 action=allow orig=r77 i/f_dir=outbound i/f_name=eth0 has_accounting=0 product=Application Control src=Winsvr2012 s_port=49359 dst=74.125.239.105 service=http proto=tcp appi_name=Google Analytics app_desc=Google Analytics is a web traffic analytics service from Google. It provides Webmasters with statistics about their website's incoming traffic, such as the traffic's volume and source. Supported from: R75. app_id=60340654 app_category=Business Applications matched_category=Business Applications app_properties=Transmits Information, Very Low Risk, Business Applications, Content Provider and Sharing app_risk=1 app_rule_id={B1962627-0961-4C6A-8536-6990833E982C} app_rule_name= web_client_type=Chrome web_server_type=Other: Golfe2 app_sig_id=60340654:2 resource=http://www.google-analytics.com/ga.js proxy_src_ip=Winsvr2012 __policy_id_tag=product=VPN-1 & FireWall-1[db_tag={B4C84FB1-7283-EF4F-BCAD-2228B3617856};mgmt=r77;date=1402094159;policy_name=Standard] origin_sic_name=cn=cp_mgmt,o=r77..pcfxuu bytes=1668 sent_bytes=1249 received_bytes=419 browse_time=0:00:00 Suppressed logs=2

Field Name	Data Type	Description	Dictionary

DLP – Data Loss Prevention

The DLP Software Blade protects sensitive corporate information from both unintentional and intentional loss. UserCheck™ technology empowers users to remediate incidents in real-time. The product field value is DLP.

Each DLP incident has a unique ID included in the log and sent to the user as part of an email notification. User actions (Send, Do not Send) are assigned the same Incident UID that was assigned to the original DLP incident log.

If a user sends an email with a DLP violation and then decides to discard it, two logs are generated. The first log is a DLP incident log with Ask User action and is assigned an Incident UID. On the user action, the second log is generated with the same UID, with the Do not Send action.

Each matched data type generates its own log. The gateway makes sure that all the data type logs of one incident indicate the same unique Incident UID and rule action (Prevent, Ask, Inform, or Detect), even if data types were matched on different rules. The common action for an incident is the most restrictive.

For example, assume a transmission matches two data types. Each data type is used in a different rule. The action of one rule is Prevent. The action of another rule is Detect. The two logs that are generated will indicate Prevent as the action. (The action implemented will be Prevent.) The log of the Detect rule will show Rule Base (Action set by different rule) in the DLP Action Reason column.

Some fields are restricted to administrators without permissions. Values for these fields are replaced in the LEA stream with ―Confidential. These are listed in the Security Management Admin Guide. They are DLP Rule Name, DLP Rule UID, Data Type UID, Data Type Name, User Action Comment, DLP Recipients, Scanned Data Fragment, Message to User, DLP Categories, DLP Words List and Mail Subject. When the LEA client uses sslca as the connection method, then the OPSEC Application Object permission profile may be set to show confidential values.

Field	Data Type	Description/Values	Dictionary
client_inbound_bytes	LEA_VT_INT	client inbound bytes	No

QoS

Quality of Service (QoS) (formerly FloodGate-1) is a policy-based solution for VPNs, private WANs and Internet links. It optimizes network performance by assigning priority to business critical applications and end-users. A QoS policy acts within the bandwidth specified on the gateway interface for the direction of traffic flow. Statistics relative to the interface direction are reported when the rule Track option is Account. Client is the host originating the connection and server is the destination host.

Field	Data Type	Description/Values	Dictionary
client_inbound_bytes	LEA_VT_INT	client inbound bytes	No
client_inbound_interface	LEA_VT_STRING	client inbound interface	Yes
client_inbound_packets	LEA_VT_INT	client inbound packets	No
client_outbound_bytes	LEA_VT_INT	client outbound bytes	No
client_outbound_interface	LEA_VT_STRING	client outbound interface	Yes
client_outbound_packets	LEA_VT_INT	client outbound packets	no
fg-1_client_in_rule_name	LEA_VT_STRING	name of the rule matching a client connection on the interface	
fg-1_client_out_rule_name	LEA_VT_STRING	see above	
fg-1_server_in_rule_name	LEA_VT_STRING	name of the rule matching a server connection on the interface	
fg-1_server_out_rule_name	LEA_VT_STRING	see above	
server_inbound_bytes	LEA_VT_INT	server inbound bytes	No
server_inbound_interface	LEA_VT_STRING	server inbound interface	Yes
server_inbound_packets	LEA_VT_INT	server inbound packets	No
server_outbound_bytes	LEA_VT_INT	server outbound bytes	No
server_outbound_interface	LEA_VT_STRING	server outbound interface	Yes
server_outbound_packets	LEA_VT_INT	server outbound packets	No

VoIP (Voice over IP)

Check Point secures VoIP traffic. If VoIP logging is turned on in the Global Properties -> Log and Alert, then SIP and H.323 events are available to LEA clients. There are Log fields for;

- Call registration event. For SIP, the Reg. IP-phones field shows the SIP URL (for example, example@checkpoint.com). For H.323 this field shows the phone number (#1234, for example)
- Call setup events (Source and Destination IP Phone).
- Media Type (audio, video, instant messaging, applications, unknown) flowing between the source and destination IP Phones.

The Information field shows messages such as H.323 Message: H.225 Setup Message. If VoIP logging is not turned on, only standard logging will take place, showing the source, destination, protocol, and so on.

Field	Data Type	Description/Values	Dictionary
dst phone number	LEA_VT_STRING	terminator IP phone SIP URL. (callee)	
media type	LEA_VT_STRING	media type of the call: e.g.: audio or video	
Registered_IP_phones	LEA_VT_STRING	IP phone SIP URL that registered in the proxy.	
src phone number	LEA_VT_STRING	originator IP phone SIP URL. (caller)	
voip_attach_action_info	LEA_VT_STRING	Attachment action information	
voip_attach_sz	LEA_VT_STRING	Attachment size	
voip_call_dir	LEA_VT_STRING	Call direction	
voip_call_id	LEA_VT_STRING	Call-ID	
voip_call_state	LEA_VT_STRING	Call state	
voip_call_term_time		Call termination time stamp	
voip_config		Call configuration	
voip_duration	LEA_VT_STRING	Call duration	
voip_est_codec	LEA_VT_STRING	Estimated codec	
voip_exp	LEA_VT_STRING	Expiration	

voip_from_user_type	LEA_VT_STRING	Source IP phone type	
voip_log_type		VoIP log type	
voip_media_ipp	LEA_VT_STRING	Media IP protocol	
voip_media_port	LEA_VT_STRING	Media port	
voip_method	LEA_VT_STRING	Request	
voip_reason_info	LEA_VT_STRING	VoIP reject reason information	
voip_reg_ip		Registration IP	
voip_reg_ipp		Registration IP protocol	
voip_reg_period	LEA_VT_STRING	Registration period	
voip_reg_port		Registration port	
voip_reg_server		Registrar server	
voip_reg_user_type	LEA_VT_STRING	Registered IP-phone type	
voip_reject_reason	LEA_VT_STRING	VoIP reject reason	
voip_to_user_type	LEA_VT_STRING	Destination IP-phone type	

Audit

Audit logs capture management related records such as records of changes made to objects in the Rule Base and general SmartDashboard usage. In NG FP3 Audit logs were made available to LEA clients via the collected log files mechanism.

Note: A list of the Operation Numbers and corresponding Operation descriptions is available in SecureKnowledge solution sk31311.

Field Name	Data Type	Description	Dictionary
Additional Info		Examples include Security Policy|Desktop Policy|etc.	
Administrator		administrator performing the operation	
Audit Status		success or failure	
FieldsChanges		specific field change information	
Machine		client host	

ObjectName	LEA_VT_STRING	application object name	yes
ObjectTable		object repository table	
ObjectType		object type	
Operation		operation description	
Operation Number		operation ID number	
product	LEA_VT_STRING	Examples include SmartDashboard, SmartView Tracker, etc..	yes
session_id	LEA_VT_STRING	the optional session name entered when logging in to SmartDashboard	
Subject		operation description	

ClusterXL Related

ClusterXL is a software-based Load Sharing and High Availability solution that distributes network traffic between clusters of redundant VPN-1 Pro Gateways, and provides transparent failover between machines in a cluster. ClusterXL uses unique physical IP and MAC addresses for the cluster member, and virtual IP addresses to represent the cluster itself.

Note: While the SmartCenter or CMA uses the virtual IP address to identify the cluster, the orig field in the logs from the cluster members has the value of the cluster member IP address and not the virtual IP address of the cluster.

Field Name	Data Type	Description	Dictionary
cluster_info	LEA_VT_STRING	see below	No
sync_info	LEA_VT_STRING	see below	

The following values are documented in the ClusterXL User Guide. Depending on the version of the firewall these may appear in message_info, sync, sync_info, or cluster_info fields. These logs typically have the action field value of ”ctl”.

General logs:

- Starting <ClusterXL|State Synchronization>.
- Stopping <ClusterXL|State Synchronization>.
- Unconfigured cluster Machines changed their MAC Addresses. Please reboot the cluster so that the changes take affect.

State logs:

- Mode inconsistency detected: member [ID] ([IP]) will change it’s mode to [MODE]. Please re-install the security policy on the cluster.

- State change of member [ID] ([IP]) from [STATE] to [STATE] was cancelled, since all other members are down. Member remains [STATE].
- member [ID] ([IP]) <is active|is down|is stand-by|is initializing> ([REASON]).

Pnote logs:

- [DEVICE] on member [ID] ([IP]) status OK ([REASON]).
- [DEVICE] on member [ID] ([IP]) detected a problem ([REASON]).
- [DEVICE] on member [ID] ([IP]) is initializing ([REASON]).
- [DEVICE] on member [ID] ([IP]) is in an unknown state ([STATE ID]) ([REASON]).

Interface logs:

- interface [INTERFACE NAME] of member [ID] ([IP]) is up
- interface [INTERFACE NAME] of member [ID] ([IP]) is down (receive <up|down>, transmit <up|down>)
- interface [INTERFACE NAME] of member [ID] ([IP}) was added
- interface [INTERFACE NAME] of member [ID] ([IP}) was removed

SecureXL logs:

- SecureXL device was deactivated since it does not support CPLS.
- SecureXL does not support unicast CPLS. Acceleration was stopped.

Reason strings:

- member ID ([IP]) reports more interfaces up
- member ID ([IP]) has more interfaces – check your disconnected interfaces configuration in the <discntd.if file|registry>
- [NUMBER] interfaces required, only [NUMBER] up

Other Check Point Products

FireWall-1 GX

FireWall-1 GX delivers Check Point's market-leading security to GPRS- (2.5G) and UMTS- (3G) enabled wireless networks.

Field Name	Data Type	Description	Dictionary
gtp_ver	LEA_VT_INT	GTP protocol version (0, 1)	
signal_type	LEA_VT_STRING	GTP Message Type	
ms_isdn	LEA_VT_STRING	Mobile subscriber ISDN number (i.e. the Telephone Number).	

apn	LEA_VT_STRING	Access Point Name which describes the Network and/or Service that the Subscriber connects to.	
selection_mode	LEA_VT_STRING	Indicates the origin of the APN that appears in the PDP context request (0, 1, 2)	
end_user_address	LEA_VT_IP_ADDR	The IP address of the Mobile Subscriber device.	
sgsn_signal	LEA_VT_IP_ADDR	SGSN IP address for signaling	
sgsn_traffic	LEA_VT_IP_ADDR	SGSN IP address for traffic (Aka User plane)	
ggsn_signal	LEA_VT_IP_ADDR	GGSN IP address for signaling	
ggsn_ traffic	LEA_VT_IP_ADDR	GGSN IP address for traffic (Aka User plane)	
GTP message info	LEA_VT_STRING	A free text used to describe errors and problems. Will appear in the "Info" column.	
n_pdus	LEA_VT_INT	Accounting information: the number of User plane packets (Aka T-PDUs) that were sent for a specific GTP tunnel.	
		Will appear in the "Info" column.	
n_bytes	LEA_VT_INT	Accounting information: the number of User plane bytes that were sent for a specific GTP tunnel.	
		Will appear in the "Info" column.	
tid	LEA_VT_STRING	GTP Tunnel ID. For GTP version 0 only.	
teid_uplink	LEA_VT_HEX	GTP uplink control Tunnel End Point ID. For GTP version 1 only.	
teid_dnlink	LEA_VT_INT	GTP downlink control Tunnel End Point ID.	
		For GTP version 1 only.	
nsapi	LEA_VT_INT	GTP NSAPI (Network Service Access Point Identifier). (An integer in the range [1,…,15]).	
linked_nsapi	LEA_VT_INT	GTP linked NSAPI. For GTP version 1 only. (An integer in the range [1,…,15].)	
mobile_country_code	LEA_VT_STRING	Mobile Country Code (MCC) of the relevant GTP Tunnel.	
mobile_network_code	LEA_VT_STRING	Mobile Network Code (MNC) of the relevant GTP Tunnel.	
mobile_subscriber_code	LEA_VT_STRING	Mobile Subscriber Identification Number (MSIN) of the relevant GTP Tunnel.	

		The MCC, MNC & MSIN together defines the International Mobile Subscriber Identity – aka the IMSI.	
GTP	LEA_VT_STRING	Used to add free text to the "Info" column in FireWall-1 GX logs.	

Interspect

Interspect is an internal security gateway that blocks the spread of worms and attacks inside your network. InterSpect segments your network into security zones, minimizing unauthorized access - intentional and unintentional. It also isolates attacks and compromised devices. Interspect can be configured to send logs to a remote SmartCenter or act as a LEA server.

Field Name	Data Type	Description	Dictionary
action	LEA_VT_ACTION	additional actions were added; bypass, inspect, quarantine, block, monitor	yes
Zone		networks that are segmented	yes
src_mac		Source MAC address	
dst_mac		Destination MAC address	
attack		attack category	no
Attack Info		additional information about the attack	no
Packet info		additional details about the packet	no

IPS-1

IPS-1 is a dedicated intrusion detection and prevention system (IDS/IPS) that helps organizations secure their enterprise network, and protect servers and critical data against known and unknown worms, automated malware, and blended threats.

IPS-1 log events are available from the IPS-1 Management Server via syslog. By Q4 of 2009 IPS-1 log events will be available via the LEA API. The product field name will be "IPS-1".

To receive events via syslog modify the /etc/syslog.conf file on the IPS-1 Management Server so that all syslog messages from facility Local5 and priority notice will be forwarded to the syslog server using the entry:
local5.notice -TAB- @<SyslogServerName>.

In the **Alert Actions** tab of **Policy Manager**, expand the **Built-in Groups**. Right-click an Alert Group for which syslog messages should be generated and select **Edit Actions**. To send syslog

messages for all alerts, right-click **all** and select **Edit Actions**. The **Edit Actions for Alert Group – all** window appears.

Edge

VPN-1 Edge appliances provide secure connectivity for remote sites, such as branch, retail and partner sites. Edge devices can be managed remotely using a Security Management Portal (SMP), SmartCenter, or Provider-1. The logs can be retrieved from the SMP or the Edge device directly via syslog. To retrieve the logs from SmartCenter, CMA, or CLM use LEA.

Edge connection logs are in standard Check Point format or if specific to Edge the format is defined in the logger.ini file in the conf directory of the SmartCenter server. Control messages have the product value ”VPN Embedded Connector” with an orig .value of the SmartCenter server.

Note: The IP address of the Edge device may be obtained via DHCP and thus may change. In this case the raw value of the orig field may be more useful than the resolved value.

Field Name	Data Type	Description	Dictionary
product	LEA_VT_STRING	The product field value is “VPN-1 Edge” or ”VPN Embedded Connector”.	
msg	LEA_VT_STRING	Description of the log defined in logger.ini file.	
rule		In firmware version 6.x (and in some cases in version 5.x) a negative rule number indicates an implied rule, e.g. Rule -4: Anti-Spoofing [5]. The connection was dropped due to the automatic anti-spoofing rules. There is a list of the rule numbers and meaning in the http://www.sofaware.com Knowledge Base.	

VSX

VPN-1 VSX (Virtual System Extension) addresses the security needs of complex environments such as data centers, POPs and large, segmented networks. VPN-1 VSX provides a set of virtual components acting as real network devices such as Firewall gateways, routers and network cables. Using these virtual components, you can create network topologies functionally equivalent to the physical networks you would build using physical devices. Each Virtual Firewall, called Virtual System, functions as a separate firewall. As packets arrive at a VSX Gateway, it selects the appropriate Virtual System to handle them. Thus instead of using multiple

Firewall/VPN Gateways each protecting a single internal network, a single VPN-1 VSX Gateway can be used. Both SmartCenter and Provider-1 can be used to manage VPN-1 VSX.

Field Name	Data Type	Description	Dictionary
orig	LEA_VT_STRING	There are Virtual Server objects without an IP like cluster members. In such objects the value of the orig field will be 0 or localhost. This may cause problems in existing LEA application that use the 'orig' field as unique identifier. In this case do not use lea_resolve_field(). Instead use the LEA log field orig_name'	yes
orig_name	LEA_VT_STRING	The Virtual Server object.	yes
origin_sic_name	LEA_VT_STRING	The SIC name of the Virtual Server object	

Endpoint

Endpoint Security is a managed solution for securing endpoint PCs. Endpoint Policy Management centrally manages desktop firewall security, intrusion prevention, outbound threat protection, and access policy enforcement. Endpoint PC firewall policy logs can be sent from Endpoint Policy Management Server to a SmartCenter/CMA/Security Management server.

Endpoint client logs are in standard Check Point format. In R70 Security Management the product name changed from Integrity to EndpointSecurity.

Field Name	Data Type	Description	Dictionary
application_ip		Example: "internal_computer6.company.com"	
application_port		Example: "53"	
attack		Attack name	
compliance_action		Compliance action	
compliance_name		Compliance rule, Example: "SecureClient Installed"	
compliance_provider		Example: "system"	
compliance_reason		Example: "file.exists.path.program.exe"	
compliance_reason_data		Example: "0"	
compliance_rule_id		Example: "2"	
compliance_type		Compliance type	
count		Example: "3"	

domain_id		The domain ID	
domain_name		Example: ”System_domain”	
endpoint_addr		Endpoint IP address	
endpoint_id		Endpoint ID	
endpoint_ip		Endpoint IP address	
event_count		Event count	
event_type		Event Type. Example: ”compliance violation”	
file_name		Example: ”ccdoctor.exe”	
file_type		File type	
im_event		IM event	
im_protocol		IM protocol	
im_userid		IM user	
integrity_av_email_from		Endpoint AV email sender	
integrity_av_email_to		Endpoint AV email recipient	
integrity_av_event		Endpoint AV scan event	
integrity_av_invoke_type		Endpoint AV scan type	
lock_level		Example: ”emergency lock”	
orig		The endpoint client address	
policy_id		The policy ID	
policy_name		Example: ”policy_restrict”	
product	LEA_VT_STRING	The product field value is “Integrity” or EndpointSecurity.	no
rule_name		The name assigned in the Integrity endpoint policy firewall policy.	No
spyware_action		Example: ”quarantine”	
spyware_name		Example: ”ToxiBackDoor 1.00”	
spyware_status		Example: ”success”	
spyware_type		Example: ”Trojan”	
user		The current user logged on to the endpoint client. Example: ”z118:n/a:10.0.0.1”	no
user_directory		User Directory. Example: ”z118”	
user_group		User Group	
version		Endpoint version	
virus name		Virus name	

Version Updates

Notes:

- This is not a complete list of all of the changes.
- See Software Support Timeline for a comprehensive list of product release dates and a support timeline.

Changes From 4.1 to NG

Release date: June 2001

New Features

- Client side LEA filtering capabilities
- New APIs to support log tracking
- New set of APIs to support access to collected files
- Log records are comprised of one or more fragments

Field Changes

Field in 4.1	Field in NG	Comments
sys_msgs	sys_message:	name change
ISAKMP Log:	IKE Log:	name change (changed in 4.1 SP3)
SPI:		Manual IPSec not available in NG, therefore the field is no longer available
Negotiation Id:	CookieI CookieR	"Negotiation Id:" is the concatenation of CookieI and CookieR, separated by a dash. There are no changes in the content, only in the meaning of the field. If the dash is there, it's in IKE phase 1, if not, its IKE phase 2. In FireWall-1/VPN-1 4.1 SP3 and above, the content will be in the msgid field rather than in Negotiation ID:
product	product	The "product" field in FireWall-1 and VPN-1 v4.1 always contained "VPN-1 & FireWall-1" for Check Point log records, and perhaps other values in log records written by vendors using the ELA interface. In NG, more than one Check Point product might want to give an opinion about a single connection. Therefore more than one value might exist in a

		single field, separated by new lines. For example, "VPN-1 & FireWall-1\nFloodgate-1\n…"
alert	alert	In FireWall-1 and VPN-1 v4.1, alerts in the alerts dictionary appear inside square brackets with a leading exclamation mark (e.g. "![mailalert]"). In NG, alerts have been simplified (e.g. "mailalert").
	UUID	VPN-1/FireWall-1 NG introduced a major change in the internal structure of the log repository, information regarding connections can now be added as time progresses. Log records are now comprised of fragments. Every log record is a chain of one or more records. Fragments are associated with a chain via their unique ID (also called UID). Every number of fragments containing the same UID is part of the same chain. All fragments of the same chain have the same UUID. The record that lea client gets may be already unified (depends on the logtrack parameter in lea_new_session) and no new fragments will arrive. If the lea client reads logs in a raw then the fragments can be unified using the UUID. Each log (fragment or unified) has UUID (it is just a field in the log record). But note if the record is already unified (CURRENT_UNIFIED_FILEID) then no new fragments will arrive (see also lea.pdf table 1-4 File Read Modes).
request		SAM value moved to sys_message field
expire		SAM value moved to sys_message field
target		SAM value moved to sys_message field
message	SYN Defender	SYN Defender values moved to new field
reason:	message_info, TCP packet out of state + tcp_flags	In 4.1 the log "Unknown established TCP packet" indicated a non-SYN packet was encountered that was not in the connection table. In NG this is logged in the message_info field or in the TCP packet out of state field.
len		not available in NG

h_len		not available in NG

File Access Changes

File Extension Completion

- In some situations the 4.1 LEA Server associated log files with extensions. For example, opening a file named "fw" would result in the opening of "fw.log" in LEA_NORMAL_FILENAME mode, and "fw.alog" in LEA_ACCOUNT_FILENAME mode.
- The NG LEA Server will only open files with exact filenames.
- When a LEA session is opened in some modes like "LEA_FIRST_NORMAL_FILEID" or "LEA_CURRENT_ACCOUNT_FILEID" where the filename is inferred from the logtrack, the LEA Server will open the appropriate file.

Files with ".alog" extension

- FireWall-1 and VPN-1 NG releases do not store the account information in a separate log file. So the ".alog" files do not exist.

NG FP1

Release date: November 2001

LEA filtering on the LEA server is available.

NG FP3

Release date: August 2002

Audit Logs

NG FP3 added support for audit log files by the collected log files mechanism.

SmartDefense

Not all of the SmartDefense logs have the product field of "SmartDefense". In general you can key on the product field where the name is SmartDefense. There are some other logs that relate to SmartDefense, but historically they have not had the product name of SmartDefense.

NG AI R54

Release date: June 2003

The following are changes in NG AI R54.

Prior to NG AI R54	NG AI R54	comments
dst peer GW: "next hop GW"	next hop	name change
	src community	new field
	previous hop	new field
	reject_category	new field. Reason for an authentication failure. Examples include "Authentication Failure|IKE failure|Gateway to Gateway authentication failure|SecureClient authentication failure"
message_info & sync	sync_info	new field to track sync related data.
message_info	cluster_info	new field to track ClusterXL related data.

Audit Log Operation Changes

In NG AI R54 some of the Operation values changed. See SecureKnowledge solution sk31311 for a list of the Operation Number and Operation relationship.

NG AI R55

Release date: November 2003

Additional fields were added for the products; Interspect, Web Intelligence, VSX, and Edge.

Field Name	Data Type	Comments
Action	LEA_VT_ACTION	new actions were added (redirect, vpnroute, bypass, inspect, quarantine, block, monitor)
Zone		new field in Interspect
Total logs		new field Excessive mechanism to accumulate similar logs, and issue only one(or few) instances of it
Suppressed logs		new field Excessive mechanism to

		accumulate similar logs, and issue only one(or few) instances of it
attack -> PMTU – TCP		"Packet info" (string) is used for reporting MSS, instead of "Attack Info
attack -> PMTU – ICMP		"Packet info" (string) is used for reporting MTU, instead of "Attack Info"
attack -> Large Ping		Packet info" (string) is used for reporting length, instead of "packet_data_len"
attack -> Syndefender		Only Individual SYN logging will be suppressed. Logs will be issued as "Attack Info" instead of "SynDefender"
attack -> HTTP Worm Catcher		"Attack Info" contains worm name. Offending URL is reported in "URL_filter_pattern_detected" (hasn't changed)
attack -> HTTP header filter		Instead of issuing "HTTP header filter matched: <user defined label>" string, the user defined label is issued as "Attack Info" instead.
attack -> CIFS Worm catcher		"Attack Info" contains worm name. Offending SMB request is reported in "CIFS worm pattern detected" (hasn't changed)
attack -> Dynamic ports		Removed "reason field" from "bad port cmd" log format. Instead, either "tried to open port lower than 1024" or "tried to open a known service port" will be issued as "attack info"
attack -> Ping of death		Removed "recurrence" log format
attack -> Teardrop		Removed "recurrence" log format
attack -> SIP		ASM SIP logs were issued in the "attack info" field without an "attack name" field. Now they are issued with either one of the following "attack name"s: "Malformed SIP datagram" or "SIP content security violation"
attack -> Port scan		Removed "scan type" field from Port scan log format. Instead it will be issued under the "attack info" field. Possible values are: "Host Port Scan" and "IP Sweep Scan"

NGX R60

Release date: August 2005

IPv6 support added. Integrity and Connectra logs are available via LEA. See the Integrity and Connectra sections above.

Field Name	Data Type	Comments
service_id		Check Point devices are Application Intelligent and can differentiate between different versions of the same protocol. This means that more than two services may be configured in the Check Point SmartCenter server database that use the same port, e.g. ssh and ssh_version_2. Currently LEA partners who use the the lea_resolve_field() function to resolve the Service field will get the first one defined in the database which is not necessarily the correct one. In the next major OPSEC SDK release the lea_resolve_field() function will resolve the Service correctly. Partners who wish to use the current SDK can start to look for a new field service_id which will be part of the next major release. If the field has a value it can be used for the Service, otherwise the port can be resolved normally from the service field.
rule_name		In NGX there is an option to define a rule name.
rule_uid		The UUID of the rule.
session_id		When an administrator logs in to SmartDashboard there is an option for entering a session name. Changes in this session can be tracked using the session_id audit log field.
fw_subproduct		For example ”VPN-1”
vpn_feature_name		For example ”IKE” or ”VPN”

Audit Log Operation Number to Operation Changes

In NGX R60 some of the Operation Number and Operation values changed. See SecureKnowledge solution sk31311 for a list of the Operation Number and Operation relationship.

NGX R61

Release date: March 2006

Anti-Virus logs are available via LEA. See the Anti-Virus section above.

NGX R62

Release date: November 2006

Field Name	Data Type	Comments
SmartDefense profile		R62 introduced SmartDefense profiles which could be applied to enforcement modules as needed.

NGX R65

Release date: March 2007

Web Filtering events are available via LEA. See the Web Filtering sections above.

Integrity log fields were added to report on blocked programs, anti-spyware, SmartDefense, AntiVirus, IM security, client error, and compliance events. See the Endpoint section above for a list of Endpoint Security logs.

Security Gateway R70

Release date: March 2009

Security Gateway R70 introduced the Software Blades architecture. See the release notes for a list of product name changes.

There is a new IPS engine in R70 and additional SmartDefense fields. The product name of SmartDefense is kept in log events.

Field Name	Product	Comments
capture_uuid	SmartDefense	IPS packet capture uuid
Confidence Level	SmartDefense	IPS protection confidence level setting
Protection Name	SmartDefense	IPS protection name
Severity	SmartDefense	IPS protection severity level setting
protection_id	SmartDefense	IPS protection ID
FollowUp	SmartDefense	IPS protection Follow-up setting
Industry Reference	SmartDefense	IPS protection industry reference
Performance Impact	SmartDefense	IPS protection performance impact setting
Protection Type	SmartDefense	IPS protection type

The Integrity product name changed from Integrity to EndpointSecurity.

Field Name	Product	Comments
Integrity > EndpointSecurity	EndpointSecurity	The product name changed from Integrity to EndpointSecurity

Additional Endpoint Security On Demand (ESOD) fields and Connectra R66 changes from Integrity Client Security (ICS) to ESOD.

Field Name	Product	Comments
ESOD_Associated_Policies	VPN-1, Connectra	Policy name
ESOD_Noncompliance_Reason	VPN-1, Connectra	Reason for non-compliance
ESOD_Rule_Action	VPN-1, Connectra	Rule action
ESOD_Rule_Name	VPN-1	Rule name
ESOD_Rule_Type	VPN-1, Connectra	Rule type
user_ics -> user_ESOD	VPN-1, Connectra	Name change from ICS to ESOD
ICS_scan_status -> ESOD_scan_status	VPN-1, Connectra	Name change from ICS to ESOD
ICS_access_status -> ESOD_access_status	VPN-1, Connectra	Name change from ICS to ESOD

The product Anti_Spam was added. There are additional email content security fields.

Field Name	Product	Comments
email_control	Anti_Spam, Web	Control

	Filtering, VPN-1, SmartDefense	
email_control_analysis	Anti_Spam, Web Filtering, VPN-1, SmartDefense	Control analysis
email_id	Anti_Spam, Web Filtering, VPN-1, SmartDefense	Email ID
email_message_id	VPN-1	Email message ID
email_recipients_num	Anti_Spam, Web Filtering, VPN-1, SmartDefense	Recipients number
email_session_id	VPN-1	Email session ID
email_spool_id	VPN-1	Email spool ID
scan_direction	Anti_Spam, Web Filtering, VPN-1, SmartDefense	File direction
src_country	Anti_Spam, Web Filtering, VPN-1, SmartDefense	Source country

Additional VoIP fields

Field Name	Product	Comments
voip_attach_action_info	VPN-1	Attachment action info
voip_attach_sz	VPN-1	Attachment size
voip_call_dir	VPN-1	Call direction
voip_call_id	VPN-1	Call ID
voip_call_state	VPN-1	Call state
voip_call_term_time	VPN-1	Call termination time stamp
voip_config	VPN-1	Configuration
voip_duration	VPN-1	Call duration
voip_est_codec	VPN-1	Estimated codec
voip_exp	VPN-1	Expiration
voip_from_user_type	VPN-1	Source IP phone type
voip_log_type	VPN-1	Log type
voip_media_ipp	VPN-1	Media IP protocol
voip_media_port	VPN-1	Media port
voip_method	VPN-1	Request
voip_reason_info	VPN-1	Reject reason info
voip_reg_ip	VPN-1	Registration IP

voip_reg_ipp	VPN-1	Registration IP protocol
voip_reg_period	VPN-1	Registration period
voip_reg_port	VPN-1	Registration port
voip_reg_server	VPN-1	Registrar server
voip_reg_user_type	VPN-1	Registered IP phone type
voip_reject_reason	VPN-1	Reject reason
voip_to_user_type	VPN-1	Destination IP phone type