Check Point

Background

The Check Point logs analysis App automatically Collect - Read - Parse - Analyzes - Reports all machine generated log data of the server and presents a comprehensive set of graphs and reports to analyze machine generated data. Use a predefined set of dashboards and gadgets to visualize and address the system software,source and targets, traffic usage, active applications, used rules and much more. This logs analysis App helps measure, troubleshoot, and optimize your servers integrity, stability and quality with the several visualization and investigation dashboards.

Steps:

1. The Check Point App is running on the firewall log.
   When adding/editing the logs to XpoLog it is mandatory to apply the correct log type(s) to each of the logs:
   a. **syslog** - all logs that the application will analyze must be tagged with **syslog** as a log type.
   b. **firewall** - all logs that the application will analyze must be tagged with **firewall** as a log type.
   c. **checkpoint -** all logs that the application will analyze must be tagged with **checkpoint** as a log type**.**

2. Once the required information is set, on each log click next and edit the log pattern, this step is crucial to the accuracy and deployment of the Check Point App. Use the following patterns for each of the logs:
   First pattern:
   {date:Date,MMM dd HH:mm:ss} {text:CheckPoint-IP} Checkpoint: {date:Deliver Date,timeDiff=0;,ddMMMyyyy HH:mm:ss;dd MMM yyyy HH:mm:ss} {text:Action,ftype=action} {text:IP,ftype=checkpointip} >{properties:Message,keysSep=:;propSep=;;,eth2 rule#_#ftype=eth2rule#_#name=Eth2 Rule;eth3 rule#_#ftype=eth3rule#_#name=Eth3 Rule;eth5 rule#_#ftype=eth5rule#_#name=Eth5 Rule;eth8 rule#_#ftype=eth8rule#_#name=Eth8 Rule;rule_uid#_#ftype=ruleuid#_#name=Rule UID;rule_name#_#ftype=rulename#_#name=Rule Name;service_id#_#ftype=serviceid#_#name=Service ID;src#_#ftype=sourceip#_#name=SRC;icmp#_#ftype=icmp#_#name=ICMP;dst#_#ftype=targetip#_#name=DST;proto#_#ftype=proto#_#name=Protocol;product#_#ftype=prodcut#_#name=Product;icmp type#_#ftype=icmptype#_#name=ICMP Type;service#_#ftype=service#_#name=Service;icmp code#_#ftype=icmpcode#_#name=ICMP Code;s_port#_#ftype=sourceport#_#name=SRC Port;d_port#_#ftype=targetport#_#name=DST Port;xlatesrc#_#ftype=xlatesrc#_#name=X Late SRC;xlatesport#_#ftype=xlatesport#_#name=X Late SRC Port;xlatedst#_#ftype=xlatedst#_#name=X Late Dst;xlatedport#_#ftype=xlatedport#_#name=X Late DST Port;NAT_rulenum#_#ftype=natrulenum#_#name=NAT Rule Num;NAT_addtnl_rulenum#_#ftype=nataddtnlrulenum#_#name=NAT Addntl Rule Num;appi_name#_#ftype=appname#_#name=App Name;app_id#_#ftype=appid#_#name=appid;matched_category#_#ftype=matchedcategory#_#name=Matched Category;app_properties#_#ftype=appproperties#_#name=App Properties;app_risk#_#ftype=apprisk#_#name=APP Risk;app_rule_id#_#ftype=appruleid#_#name=App Rule ID;app_rule_name#_#ftype=apprulename#_#name=App Rule Name;web_client_type#_#ftype=webclienttype#_#name=Web Client Type;web_server_type#_#ftype=webservertype#_#name=Web Server Type;resource#_#ftype=resource#_#name=Resource;product_family#_#ftype=productfamily#_#name=Product Family;proxy_src_ip#_#ftype=proxysrcip#_#name=Proxy SRC IP}

   Second Pattern:

{date:Date,MMM dd HH:mm:ss} {text:CheckPoint-IP} {text:Device}: {date:Deliver Date,timeDiff=0;,ddMMMyyyy HH:mm:ss;dd MMM yyyy HH:mm:ss} {text:Action,ftype=action} {text:IP,ftype=checkpointip} <{text:Network Interface} {properties:Message,keysSep=:;propSep=;;,eth2 rule#_#ftype=eth2rule#_#name=Eth2 Rule;eth3 rule#_#ftype=eth3rule#_#name=Eth3 Rule;eth5 rule#_#ftype=eth5rule#_#name=Eth5 Rule;eth8 rule#_#ftype=eth8rule#_#name=Eth8 Rule;rule_uid#_#ftype=ruleuid#_#name=Rule UID;rule_name#_#ftype=rulename#_#name=Rule Name;service_id#_#ftype=serviceid#_#name=Service ID;src#_#ftype=sourceip#_#name=SRC;icmp#_#ftype=icmp#_#name=ICMP;dst#_#ftype=targetip#_#name=DST;proto#_#ftype=proto#_#name=Protocol;product#_#ftype=prodcut#_#name=Product;icmp type#_#ftype=icmptype#_#name=ICMP Type;service#_#ftype=service#_#name=Service;icmp code#_#ftype=icmpcode#_#name=ICMP Code;s_port#_#ftype=sourceport#_#name=SRC Port;d_port#_#ftype=targetport#_#name=DST Port;xlatesrc#_#ftype=xlatesrc#_#name=X Late SRC;xlatesport#_#ftype=xlatesport#_#name=X Late SRC Port;xlatedst#_#ftype=xlatedst#_#name=X Late Dst;xlatedport#_#ftype=xlatedport#_#name=X Late DST Port;NAT_rulenum#_#ftype=natrulenum#_#name=NAT Rule Num;NAT_addtnl_rulenum#_#ftype=nataddtnlrulenum#_#name=NAT Addntl Rule Num;appi_name#_#ftype=appname#_#name=App Name;app_id#_#ftype=appid#_#name=appid;matched_category#_#ftype=matchedcategory#_#name=Matched Category;app_properties#_#ftype=appproperties#_#name=App Properties;app_risk#_#ftype=apprisk#_#name=APP Risk;app_rule_id#_#ftype=appruleid#_#name=App Rule ID;app_rule_name#_#ftype=apprulename#_#name=App Rule

Name;web_client_type#_#ftype=webclienttype#_#name=Web Client Type;web_server_type#_#ftype=webservertype#_#name=Web Server Type;resource#_#ftype=resource#_#name=Resource;product_family#_#ftype=productfamily#_#name=Product Family;proxy_src_ip#_#ftype=proxysrcip#_#name=Proxy SRC IP}