Logging & Monitoring; Events & Reports

R80.10 - Review

Daniel Noel, Security Engineer
US : Mid Atlantic : PA SLED
20180705

>> A. Review & Preparation<<

To know where you are going, you must know where you came from; amazingly true in life and just as true in business agility. IT infrastructure activity logging has proven to be vital for business accountability. One can imagine that tracking access to business resources is crucially important especially with today's cyber ecommerce & system auditing. Surprisingly knowing whom is accessing those business resources and finding the unknown, or what may be lurking in the business assets is essential in governing the IT business. The legal, compliance, and longevity of business may come down to how well the IT may detect and track those undesired activities which occur outside business parameters. Having the right security controls, detections, & preventions, without the right tracking tools would prove pointless with no accountability of the business DATA or PII to which the IT Security Administration was chosen to be the shepherd.

Implementing Check Point Security, ensuring Logging & Monitoring are deployed at the beginning will serve the security administration well from the start. Understanding the variety of deployment models may change hardware & licensing, however the same steps to ensure Logging & Monitoring configuration and limitations are reviewed will remain the same. Performance factors and capacity of the devices enforcing the business security policy is critical, monitoring systems requires CPU cycles and logging at the varying security inspection levels will drive logging volume, all need to be considered during the planning stages. Check Point Smart1 dedicated management appliances all are rated so customers can align the right product to match their business needs. Decision must be made to elect which topology, combining Smart Management with Smart Logging or do you segregate these services. The same question lies with Smart Event/Reporting, combining all components into a single platform works and performs, scaling to the solution delivering the needed performance may require dedicated hardware to match desired performance.

Deciding which model will have several influences, no two customers profile will ever be the same, sizing the right configuration lies largely with knowledge of the customer's environment. Important metrics to aid in proper sizing LOG server remain as # of daily

Logs, # of peak Logs / second and active log retention for reporting. Check Point has attempted to streamline the selection process with their Smart1 Appliance offering, outlining several key sizing requirements. Existing Check Point customer (pre R80), using the log utility "CpLogInvestigator" will provide results for the existing LOG file (ref-CPLogInvestigator) displaying what logs are occurring for the inspections blade configured. Realize, if the existing Security Gateway (SG) isn't performing a particular inspection or logging then that inspection log will not be recorded within the utility output for review. Customers may enable those features or modify the rule base to include the LOG entries during the LOG Investigation with caution (evaluation license may be necessary). Adding additional work load on the SG that is already running high in load, may find an operation impact to services. Non-Check Point and Existing-Check Point customers may utilize the **Security Check Up** service to assist in sizing SG & LOG volume within their environment. The **Security Check Up** option is an excellent way for all customers to see potential missing inspections, unknown activity, and logging levels with Advance Threat activities.

(ref:CPLogInvestigator) ref SK87263

[Expert@XXXXXXXX:0]# CPLogInvestigator -a -m -p

Thank you for using log investigator tool.
==========
Start reading log file: /opt/CPsuite-R77/fw1/log/fw.log
.....
Reading log file is DONE.

Total scanned 3050306 logs out of 3050306 logs in file
Scanned logs dates are from 23-07-2015 23:58:49 to 24-07-2015 16:30:19
==========
Product log statistics (Per Day):
- *Anti Malware : 16430*
- *Application Control : 1748816*
- *Connectra : 129*
- *Security Gateway/Management : 49*
- *SmartDefense : 190*
- *URL Filtering : 294281*
- *VPN-1 & FireWall-1 : 2370107*

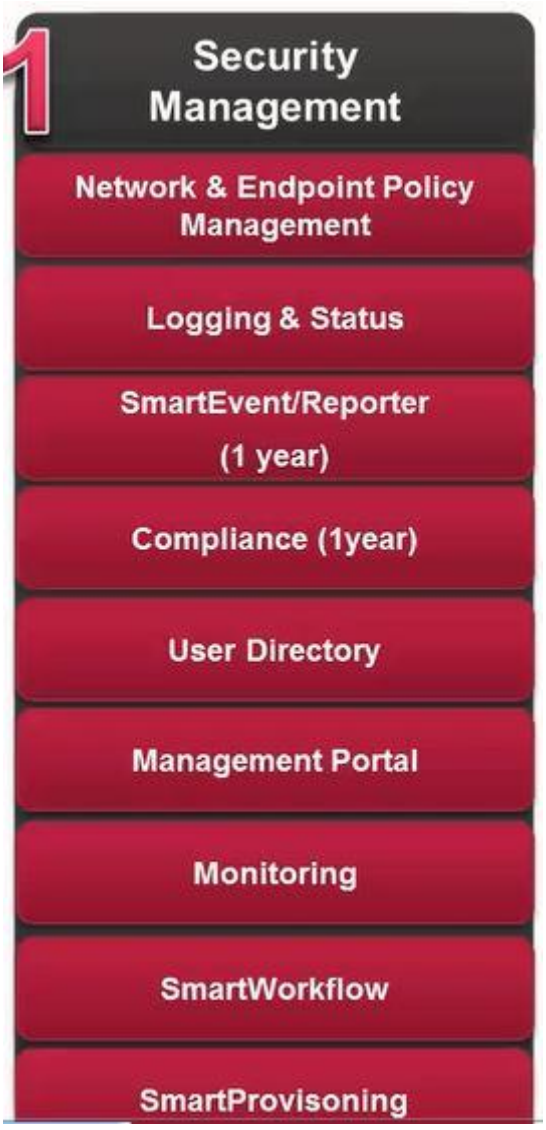
Total logs per day:

Date	GB	Count
2015-02-25	0.0333	255434
2015-02-26	0.0456	344836

(ref-1A:END)

Additional activities that will impact the volume of logs are System "Audit" Events; Access Control logging may include Application, URL, Content, & VPN or Remote Access activities; Threat Prevention profile include Anti-Virus, Anti-BOT, Intrusion Protection (IPS) & Threat Emulation/Extraction. As businesses add detections and preventions, increasing the Security Activity Visibility will proportionally increase the Logging activities. Each of these inspection Blade technologies will have their own license requirements beyond from the Smart Management license.

Check Point changed Smart Management license to a nearly inclusive offering as possible compared to recent past offers. With the right Smart Management tier purchase, supporting the # of SG's in the SMS package or the # of SG's & domains in the MDMS package, all of the basic Smart Management Blades are included (**SMS-LICENSE**). With a SMS or MDMS package, the Smart Event / Reporter & Compliance are considered more like a service and the 1st YEAR cost are included in the initial purchase. (*Note: MDMS cannot support Smart Event/Reporter imbedded, and requires a dedicated Smart Event/Reporter server. Check Point Account Services will provide the Dedicated Smart Event/Reporter license as required.) Customers that elect to deploy a Dedicated Smart Event/Reporter, this license will remain as perpetual not requiring annual service fee.

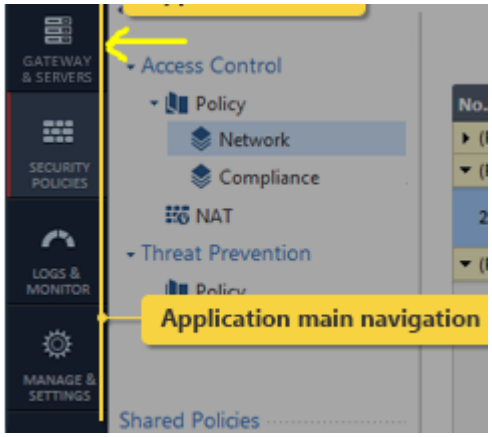


(SMS-LICENSE) Management Blades *courtesy of Check Point Account Service*

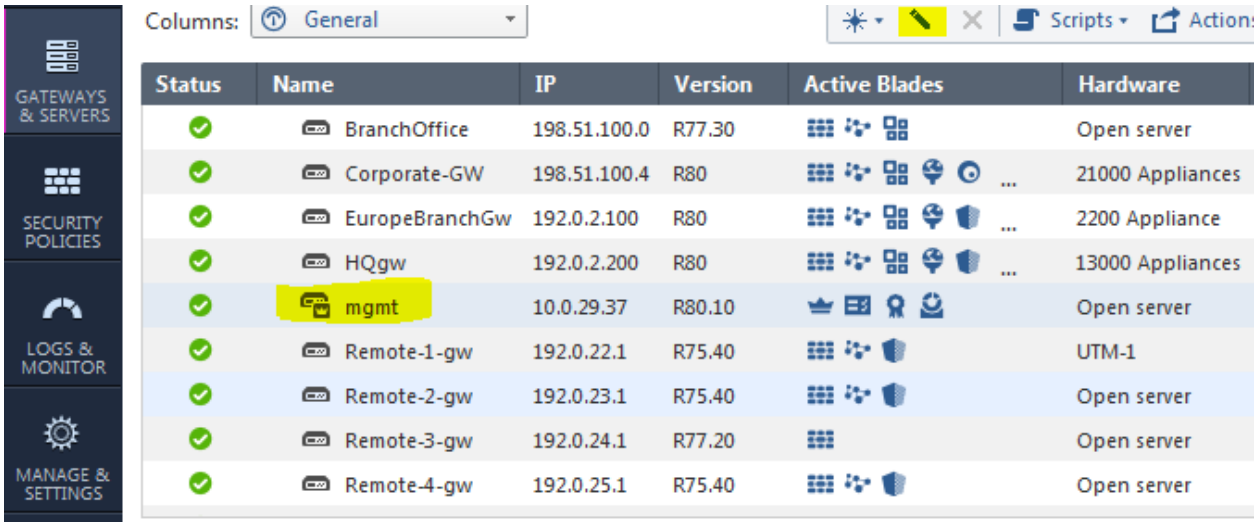
>>LOGGING ACTIVATED<<

Since R80, sizing Smart Logging & Smart Event/Reporter on the same appliance no longer demanded twice capacity for indexed Data recording. They will now share the log

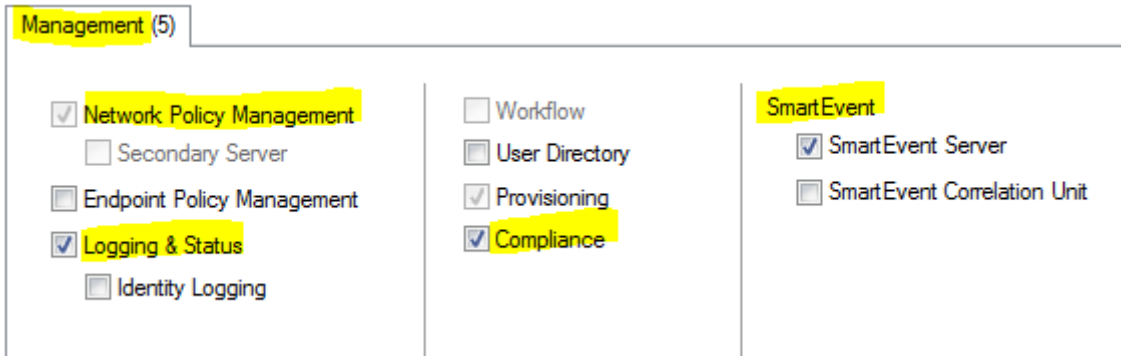
entries with separate index tracking. To enable Smart Logging, Smart Event, locate the Management Object within the “Gateway & Servers” Application Main Navigation window-pane (R80-MAIN-APP) and select. Once the “Gateway & Server” pane of glass was selected, locate the MGMT object, and edit the object to view the Management blades activated. (*Note: there are multiple ways of acting on Management Blades for the SMS, as displayed in (**Gateways&Servers**) or at the bottom right pane there is a Hyper-Link labeled as “Activate Blades”. Selecting either method will result in the same desired results, the MGMT General Property License Activation pane (Management-General-Properties).



(R80-MAIN-APP) *Application Main Navigation, click “Gateway & Servers”



(Gateways&Servers) *Select “mgmt.” and click “edit” icon



(Management-General-Properties) *Object License Activation Pane

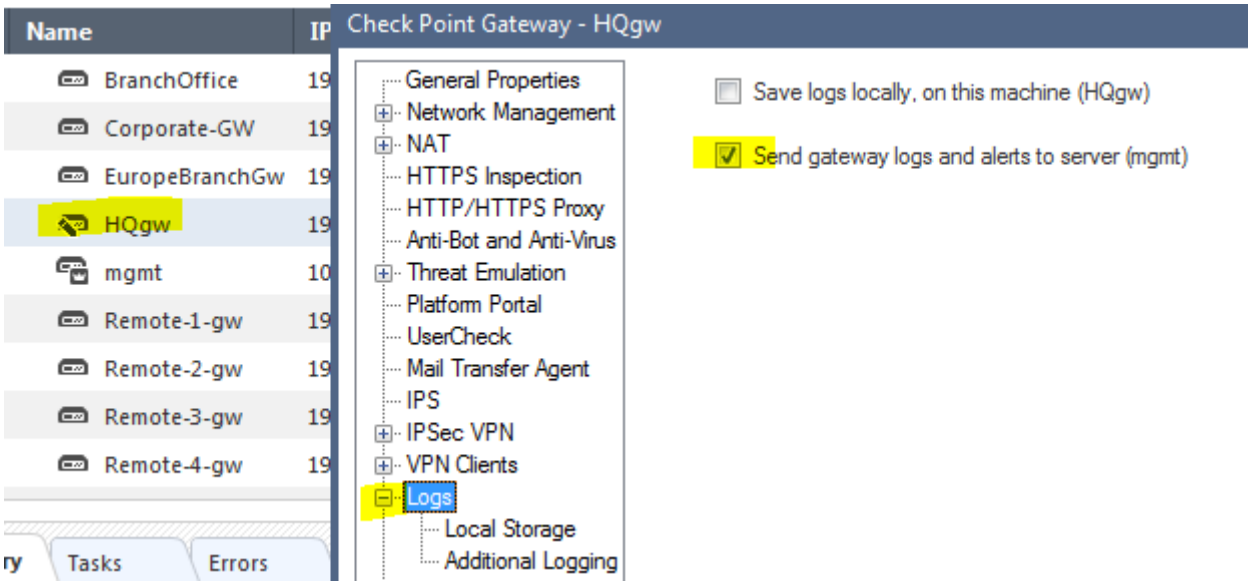
Now that Management Blades (SmartLog & SmartEvent) are enabled by selecting each product, review the SG "Logging": properties to ensure the desired Logging Server is accurate (SG-LOGS). When a dedicated log server is deployed, select the correct Log Server on the SG Object at the "Logs" pane, it is possible to send logs to more than one destination.
Monitoring Blade as part of Smart Management is included, mentioned earlier with the current license package. The security administrator will need to enable "Monitoring" on the particular SG's by activating the blade on General Properties "Network Security" tab (SG-Monitoring). On any SG's that is already experiencing HIGH CPU utilization, careful thought on enabling "Monitoring Blade" since it will add additional CPU load. The additional Traffic Connections & Traffic Throughput tracking metrics will provide the security administrators live & history counters from the SG gateway usage trends assisting SG is meeting environment as needed. Knowing how the traffic is trending for the enforcement–point will allow better reporting for the business requirements (Monitoring:CommonServices).

Once the Management & SG objects options are correctly selected and enabled perform the "Install Database" located on the "MENU" of the main title bar (Install-DATABASE).

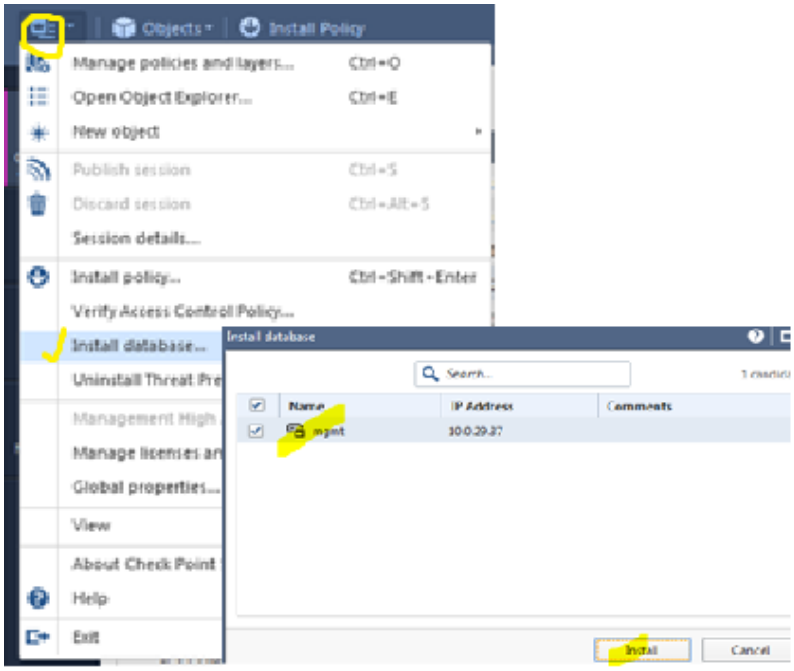
Those whom anticipate or plan on utilizing 3rd party SIEM log collector, a OPSEC LEA (SK108282) connection should be used as a reference article. Additionally Check Point advanced the support with 3rd Party log collectors using "Log Exporter" (SK122323) as an easy / secure method for exporting logs over syslog.

To manage Smart Event, select "+" to create a "New Tab" and locate the "SmartEvent Settings & Policy" under the "External Application" section (Event-Policy).

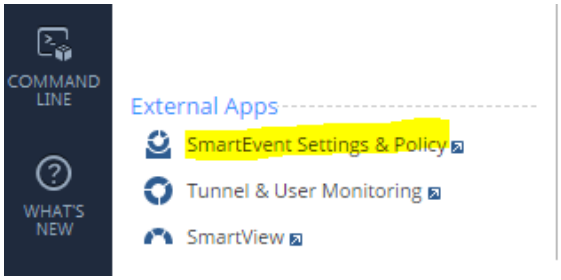
Reviewing the settings



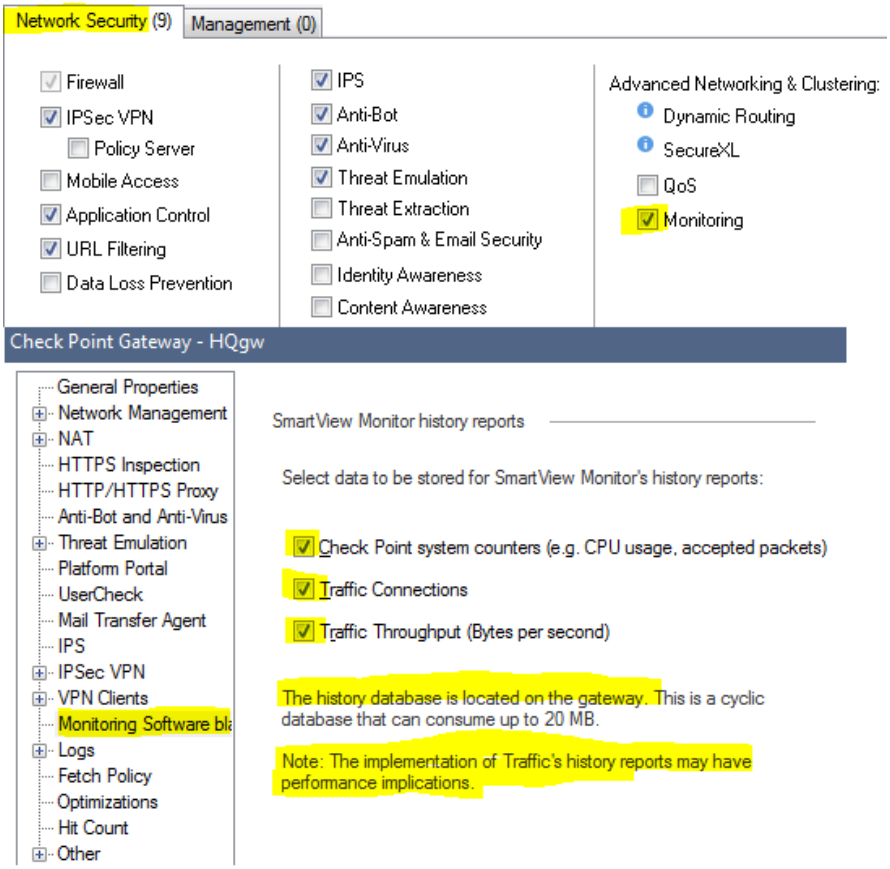
(SG-LOGS)



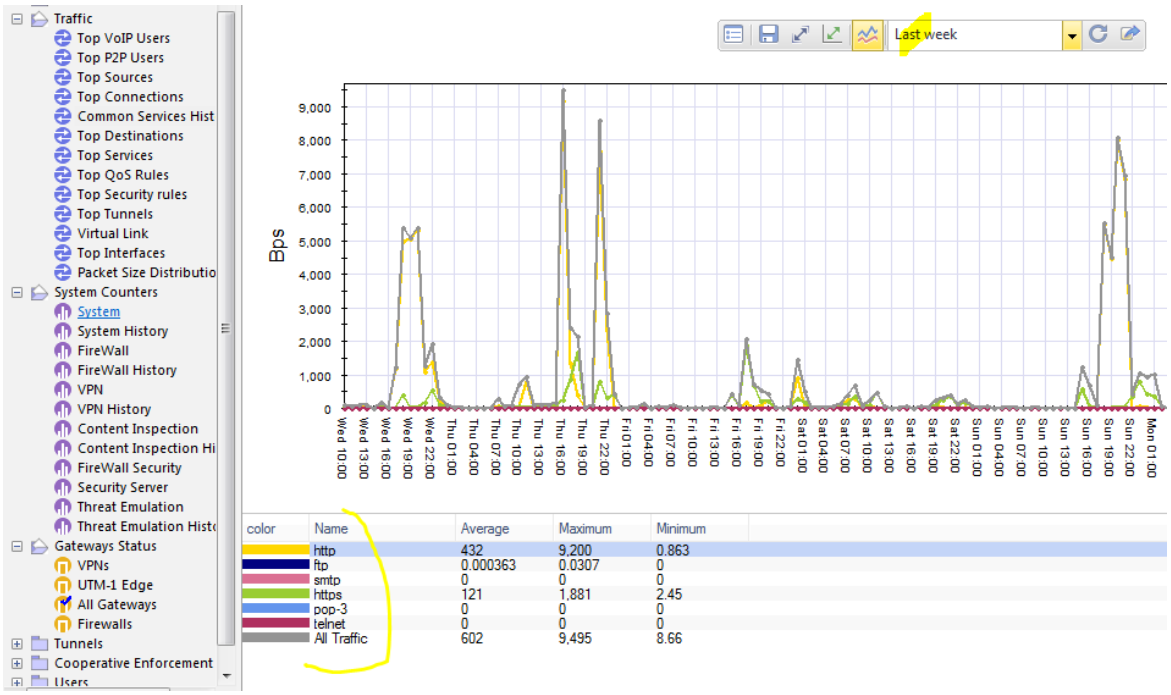
(Install-DATABASE)



(Event-Policy)



(SG-Monitoring)



(Monitoring:CommonServices)

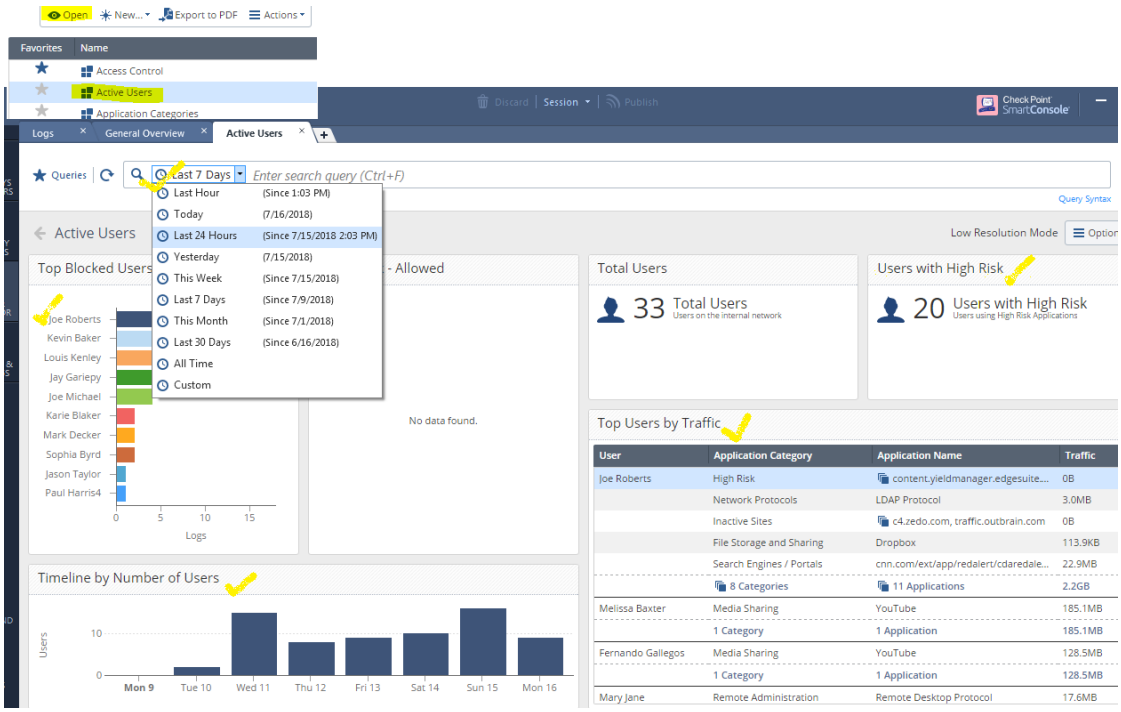
>> B. LOGS & REPORTS <<

While working within “Logs & Monitoring” located off the R80 Main Application navigation (R80-MAIN-APP) there are several default tabs “Logs”, “General Overview”, “New Tab”, each have unique values and all may be restored (if closed) by selecting the “+” for “New Tab”. Within the “New TAB” view, restoring SmartLog, or General Overview can be completed along with further views including AUDITS. Audit view allows an approved user to search and report on actions performed by Smart Console (GUI clients to manage the Security Management Server).

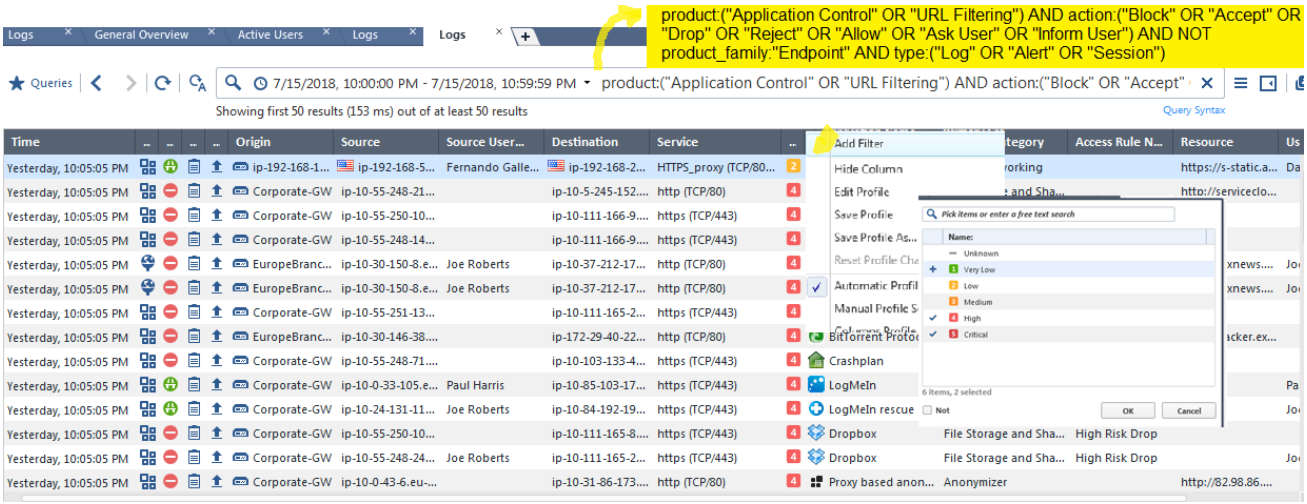
Working in the “New” tab screen there are *Favorites, *Recent, *Views, & *Reports screen options. *Favorites & *Recent are used to view the most popular or recent actions commonly used for the account. Account TASK action include *Archive, you’ll find completed reports that were exported. In the Scheduled folder, once a “Schedule Report” or “Action” is performed, this will be the location for that TASK.

>> B.a Views <<

Both Views & Reports hold predefined and customized category of view(s) & report(s). The view is an interactive dashboard comprised of multiple clickable widgets, creating customizable view, providing the administrator an account of network of events. Classic example “Active Users” view (Active-Users-View)
, more specifically “Top Blocked Users”. Open “Active Users” and review the general view provided for such active users including the “Blocked” users.



(Active-Users-View)



(Query Example1)

Further detailed review a widget listed can be drilled down by double clicking, one may choose to review the Logs of the “Users with High Risk” investigating this activity. Another focus view could be the user activity for example “Joe Roberts” having twice the BLOCKs then other users. Generally there is a time or date of concern, where you can drill down to the last 30 days down to the last hour, or create your own range. The flexibility will allow all with privileges to drill down to the view necessary creating the query syntax for even future use or further customization (Query Example). Further refinement of the DATA / LOGS can continue with the FILTERING actions of any of the COLUMNS. First “Right Click” the column for example the “RISK” column, select “Add Filter” to get the option field. Once you decide which options to include or exclude, the display of LOGS will be further refined for analysis. Adding the RISK LEVEL filter attribute of “HIGH” and “CRITICAL” will narrow the log displayed as selected.

Custom View Creation, while all the flexibility in creating the exact view is available, performing the required steps can quickly become over-whelming. All though this may seem like a basic suggestion, hoping that you see the value in what is already created by starting with an existing view. Check Point R80 allows the administrator to edit existing canned Views, choose the View and perform the CLONING option under “ACTIONS” drop down menu. Once the cloned VIEW is created and “OPEN”, at the upper right side of the display, click the “Options” button and choose the function from “Edit”, “View Filter”, or “View Setting”. Edit option will allow the modifications to tables viewed, charts options, basically it may completely be re-worked. Here the admin can re-create the view, you don’t need to re-invent the view, so take advantage of what is already created to get you started, refine to make it as desired.

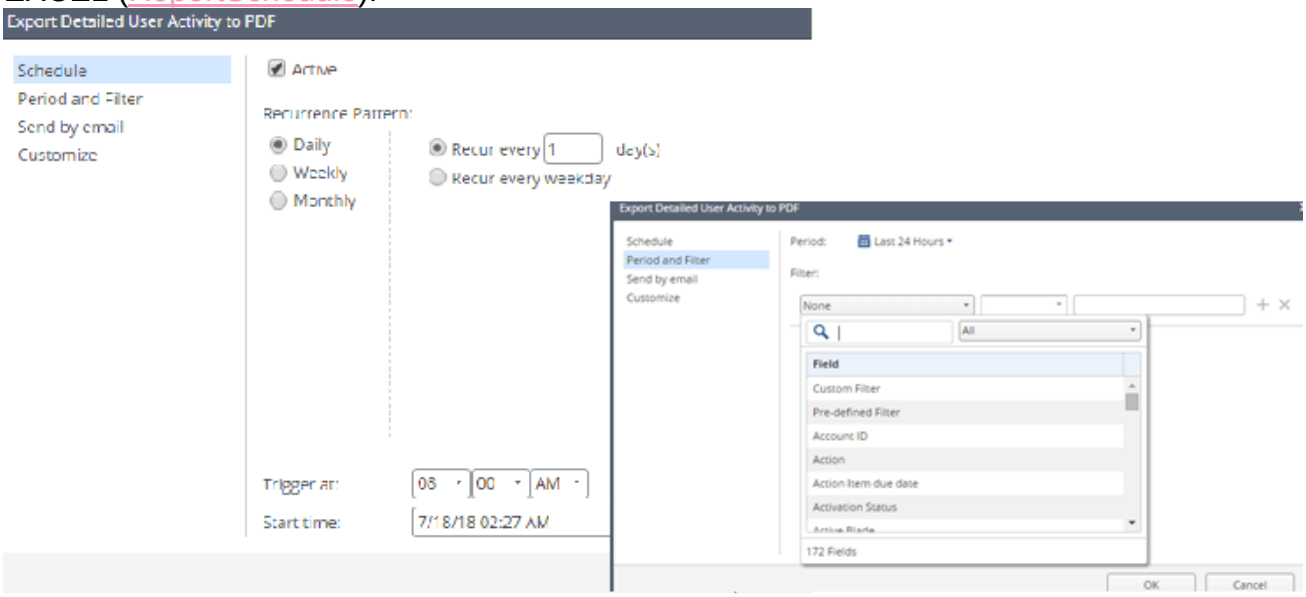
>> B.b Reports <<

Custom Report Creation are equally as configurable like custom Views, with the same process, and basic choices. The differences are the basics between REPORTS and VIEWS, defining a detailed view with widget or creating the detailed report.

Security Administrators will utilize Reports for critical informative messaging cluing in those managing IT operations that must react to RISK. Scheduling Reports (or Views) provides historical structure and consistency to those tangibles IT functions. Classic

example would be ANTI-BOT & VIRUS (Threat Prevention) report, schedule a report and have it delivered to the team managing desktops / servers / OS structured devices. Similar other behavior based detections will prove its power detecting HIGH RISK applications or WEB access.

Manually or scheduled the report task, creating the report manually simply open the report, where you may export to PDF or EXCEL. To Schedule the Report, selecting the report of interest, click the drop down “Actions” menu and choose Schedule PDF or EXCEL (ReportSchedule).



(ReportSchedule)

The TOP page will provide the scheduling, a one-time report, or will it be ran on some order of recurrence? Is the schedule ACTIVE or not? The report filter provides further refinement including the period of the report.

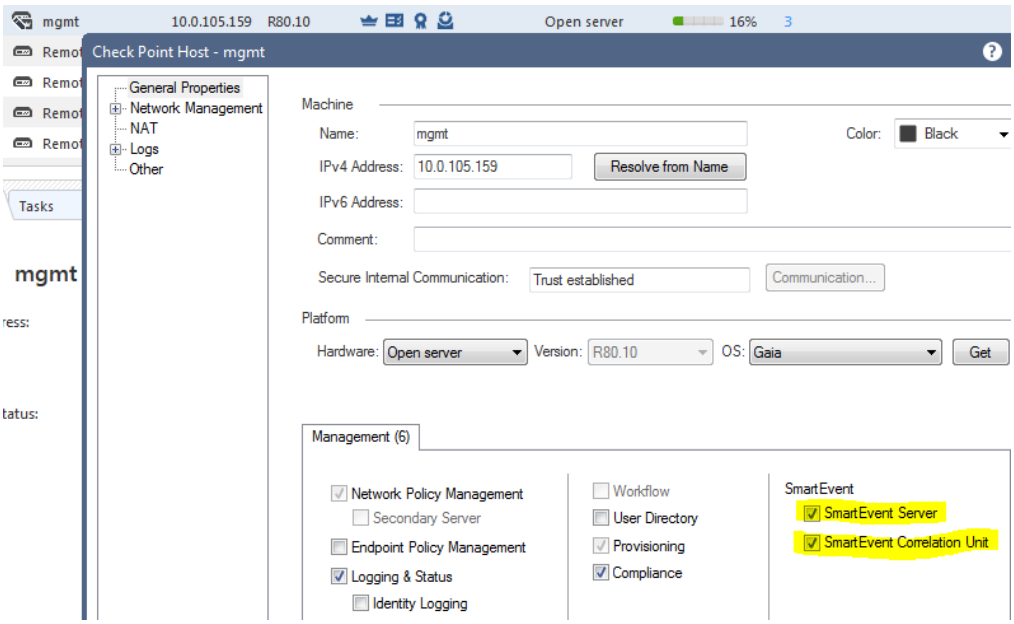
Using Checkmates Community will add to any Check Point Security Administrator arsenal or resources for questions, configurations, scripts, and filtering queries. Registering with Checkmates will utilize the same Check Point UserCenter credentials. Additional wealth of knowledge for all Check Point Secure Knowledge may be searched in the Support Center website.

>>C Smart Event <<

Check Point Smart Event has evolved over the last several years without losing the ultimate intention from the beginning. The Security Administration intelligence is elevated along with simplification and speed to combat the cyber threats surrounding or inside threatening the business intellectual property which the investment was deployed to protect. Smart Event provides centralized, real-time event correlation of log DATA. With SmartEvent, security teams no longer need to comb through the massive amount of data generated by the devices in their environment. Instead, they can focus on deploying resources on the threats that pose the greatest risk to their business. Analyzing security events of perimeter, WEB security GW, utilizing Check Point Blade Security Intelligence in real-time is AI before AI was cool. That statement may be a little presumptuous, yet the key to uncovering all this raw power, security intelligence is enabling the Security Blades for inspections along with enabling Smart Event and logging.

Smart Event & Correlation Unit as part of R80.xx Centralized Management product offering. It is as easy as enabling the Security Management Smart Event License (SmartEventActivation) to begin the deployment of Event Analysis. Sizing for Smart Event along with the number of reports, and schedule reports, or smart logging will all have an effect on the systems performance. As the business grows, the security position will follow, increasing requirements on all aspects respectfully including the security solutions.

Check Point scalable design to manage millions of logs was never intended to be performed on a single platform. Deploying a distributed architecture for Smart Event, Smart Logging or some combination of the two will provide the flexibility to fit the business requirements & budget. With a distributed architecture, Smart Event can be installed on a single server, but has the flexibility to spread processing load across multiple correlation units and reduce network load. Distributed licensing is a perpetual license model, removing the annual cost model from the Centralize Management offering.

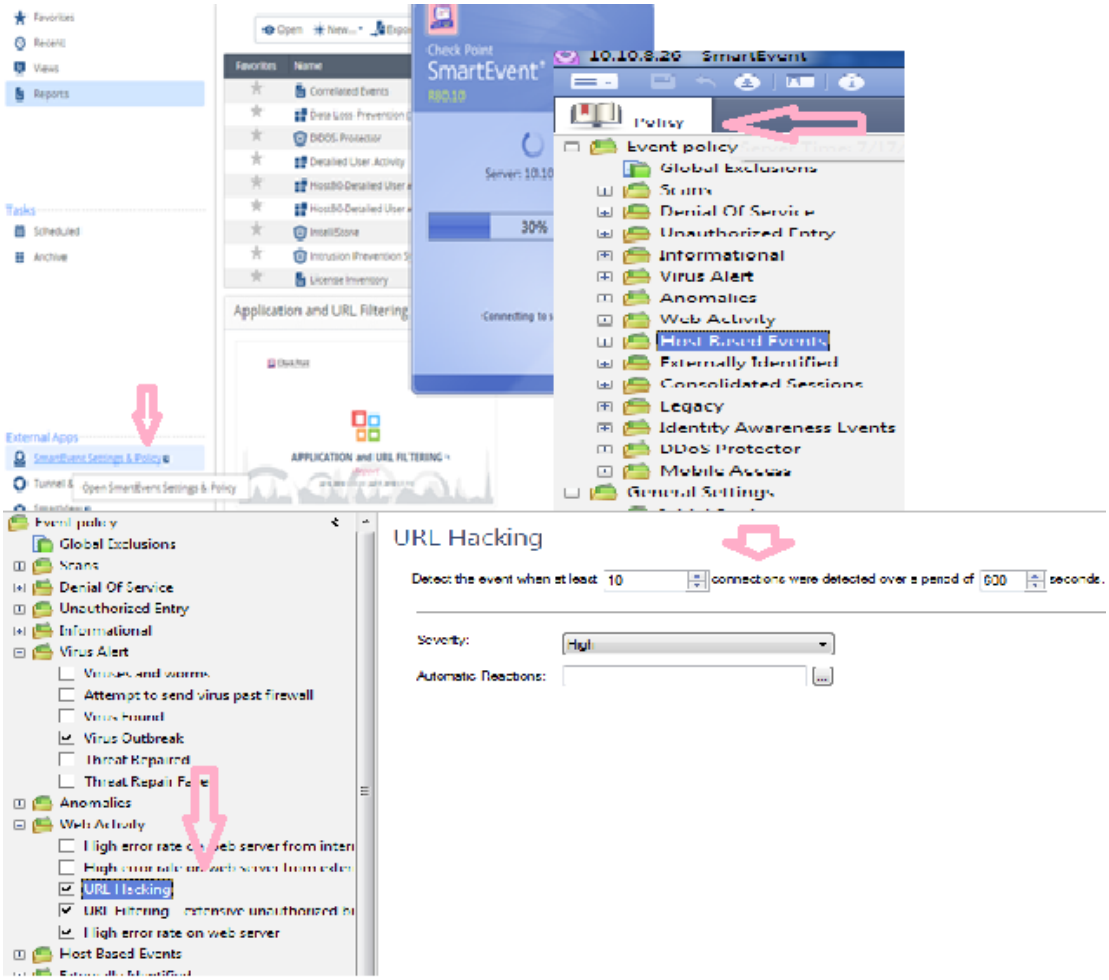


(SmartEventActivation)

Smart Event performs real-time event correlation based on blade inspection pattern log anomalies and previous data, as well from predefined security events. Once installed on the network, Smart Event has an intelligent, self-learning mode where it automatically learns the normal activity pattern for a given site and suggests policy changes to reduce false-alarm events. Smart Event is able to zero in on threats that pose greatest risk to the enterprise.

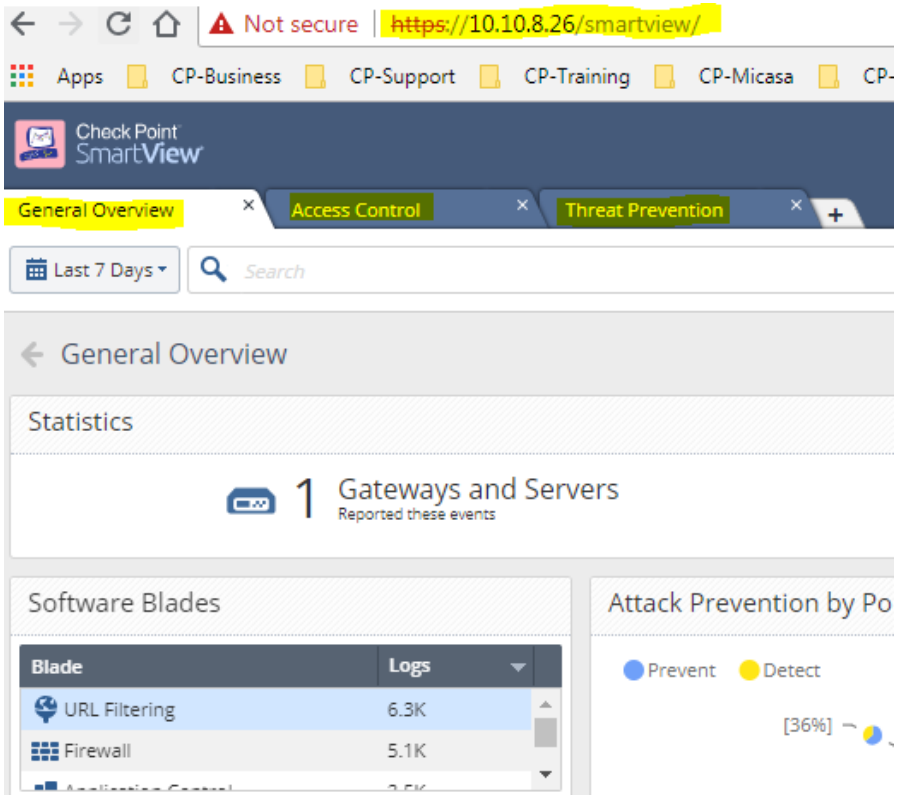
Administration of Smart Event thresholds by assigning severity levels to event categories, choose to ignore rules or set triggers on specific servers and services, greatly reducing the number of alarms or events. To make these adjustments, from the “LOGS & MONITOR” application window pane, create a “NEW TAB” if one isn’t already there. Under the “External Apps” section of the pane, there will be three listing with one “SmartEvent Settings & Policy”, click this app to open the Smart Event GUI Client (SmartEventPolicy). As the GUI window opens, the list of configurable “Event Policy” is

displayed, along with “Advance Settings” where profile of the policy is set. Expanding one of the Events like “Web Activity” provides the configurable triggers as displayed. In best practice, choose to copy Event Definition so modifications may be made on the copied version. Once the changes are made, disable the original Event by unchecking the box. At the TOP menu, install Smart Event policy to complete the changes.



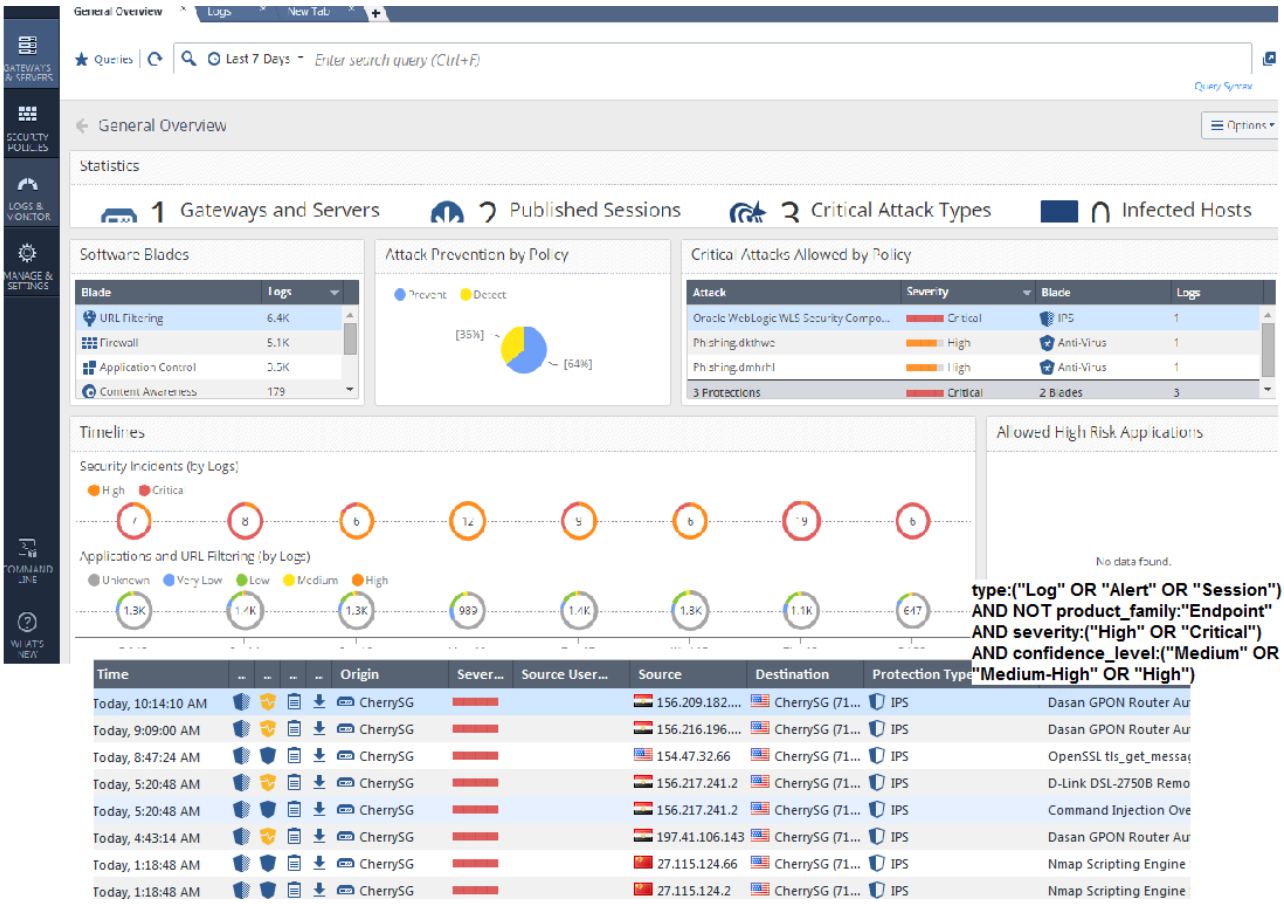
(**SmartEventPolicy**)

There are a number of Smart Event self-training materials (YouTubeRef) that more details may be found which will include many of the features including Logging, Reporting, and Views, leading us to the SmartView feature of Smart Event. The WEB access to the SmartView Client access will extend the vision throughout the essential personnel without requiring the Smart Console installation. Smartview may be accessed using the WEB browser with the address of the Management/Smartview (WEB Smartview) address. Accessing Smartview WEB pane requires credentials, once in the view, the user will have similar activity views like with the client including “General Overview”, “Access Control”, “Logging”. Even further advancements were added in the Smartview WEB portal with the release of R80.20M1 version (SK12343).



(WEB Smartview)

Although there are many views & reports available inside R80.x “Logging & Monitoring” application pane, the “General Overview” could be the initial pane used. Providing quick clickable widgets or filters in various categories finds itself as the top viewing Smart Analysis (General Overview) working screen. The VIEW can be customized, by working from a copy, double-clicking on the various windows will deliver a filtered LOG view in a TAB for details analysis. Classic example are any of the STATISTICS widgets will deliver the filter narrowing the focus or the Timeline Threat Rings, demonstrated below with the filter output.



(General Overview)

Taking time to build your comfort working within each of the “Logs & Monitoring” Application will deliver powerful messages and insight of the cyber challenges. The message continues to get stronger by showing the threats avoided or stopped, and those risk that requires mitigation. Many views producing reports on usages, and activity allows business owners to make decisions best for the business.

Many references to those SK articles, Checkmate Community, video’s and documents are found on the following pages.

References:

SK98126 - Best Practices - Configuration of logging from Security Gateway to Security Management Server / Log Server
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk98126&partition=General&product=Security

SK42952 - Configuring /etc/hosts on cluster members
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk42952

SK98977 : 'cpstart' command does not start Check Point services
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk98977

SK80720 : SmartEvent Performance Tuning Guide
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk80720

SK112797 : R80 / R80.10 Logging Capacity Performance Improvements
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk112797

R80.10 Release Notes
http://dl3.checkpoint.com/paid/88/88e25b652f62aa6f59dc955e34f98d5c/CP_R80.10_ReleaseNotes.pdf?HashKey=1531254397_c0c2e2ad40e22048069f4032705bfc4c&xtn=.pdf

SK87263 : SmartEvent Sizing Guide - R77.x
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk87263

CPLogInvestigator Reference
https://community.checkpoint.com/ideas/1041-useful-command-for-log-size-investigation

SK114114 : Disk space management tools do not delete logs from previous Security Management versions
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk114114&partition=Advanced&product=SmartConsole

SK108282 : How to configure OPSEC LEA to talk to Splunk
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108282&partition=Advanced&product=Multi-Domain

SK122323 : Log Exporter - Check Point Log Export
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323

SmartConsole and SmartView Query Language
https://sc1.checkpoint.com/documents/R80.10/SmartConsole_OLH/EN/html_frameset.htm?topic=zfFmGvPiAIUaJhQr-pxhDQ2

Check Point R80.10 Logs and Monitor Pane
https://community.checkpoint.com/videos/5769-check-point-r8010-logs-and-monitor-pane-reporting-functionality

Check Point R80.10
For more about this release, see the R80.10 home page http://supportcontent.checkpoint.com/solutions?id=sk111841

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=54830
To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com

YOUTUBE
Check Point R80.10 Logs and Monitor Pane
SmartLog and SmartEvent - CP R80.10 Lab 7.1
SmartEvent, Report, SmartView and Gateway Portal - CP R80.10 Lab 7.2

