YOUR KEY TO INTERNET SECURITY

User Guide
Check Point Analytics App by QOS

Version: 1.0.3
Date: 30 December 2015

Table of Contents

IMPORTANT INFORMATION

Our objective to make the best possible Splunk app for Check Point and therefore we are always listening to our customer's feedback.

If you find any problem while using our app or you need any assistance to set up LEA we are always there to help you.

Please feel free to mail us at splunk@qos.co.in and we will get back to you in less than 48 hrs.

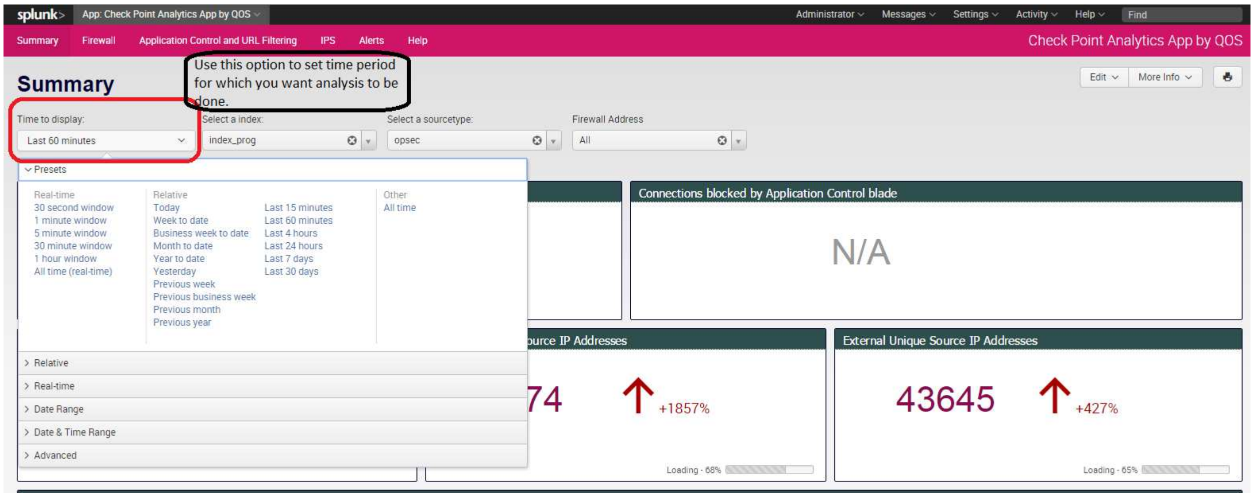
If you are emailing us for any support related matters please provide as much information as possible so that our team can help you. Make sure you mention the Splunk version, OS details, Check Point LEA version etc when trying to reach us for technical help.

COMMON SETTINGS

When you login to **Check Point Analytics App by QOS** you may want to choose appropriate settings as per your Splunk Deployment. Following is the list of settings which may require your attention before you start getting analytics from your Check Point logs.

Time to display:

Here you can choose the time period for which you want Splunk to analyze the data from Check Point. By default the time is setup to last 60 mins.



Use this option to set time period for which you want analysis to be done.

Time to display: Last 60 minutes

Select a index: index_prog

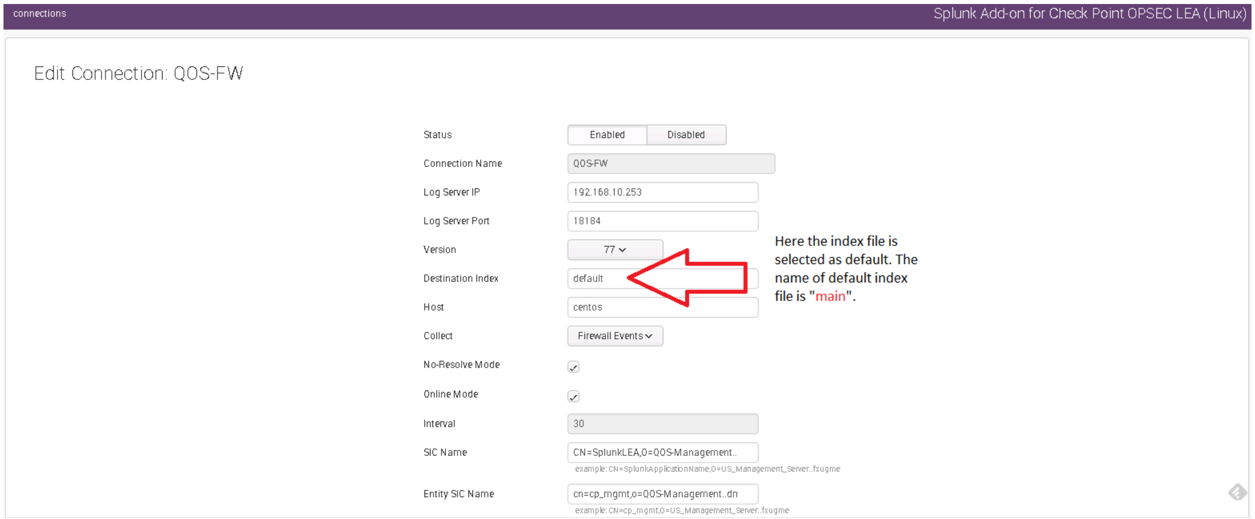
Select a sourcetype: opsec

Firewall Address: All

Select an index:

When you have installed Check Point LEA client on your Splunk Enterprise you would have chosen some index file to store Check Point index data. You need to select that index file from this dropdown list. This dropdown list will display all index files (except hidden index files like _internal etc).

Here is the screenshot of Check Point LEA App which displays its index file setting.

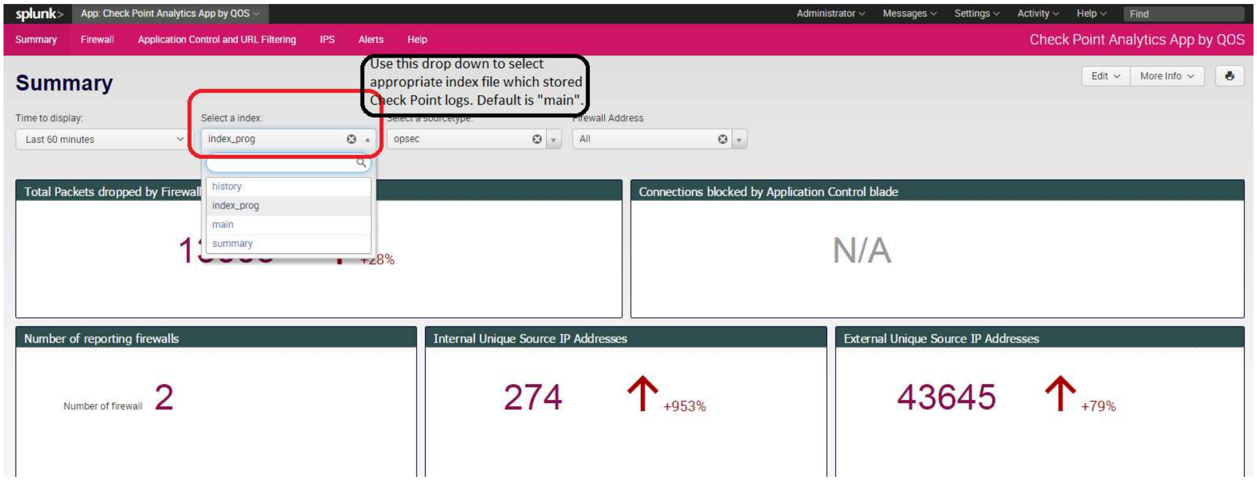


Edit Connection: QOS-FW

Status: Enabled | Disabled
Connection Name: QOS-FW
Log Server IP: 192.168.10.253
Log Server Port: 18184
Version: 77
Destination Index: default
Host: centos
Collect: Firewall Events
No-Resolve Mode: ☑
Online Mode: ☑
Interval: 30
SIC Name: CN=SplunkLEA,O=QOS-Management..
example: CN=SplunkApplicationName,O=US_Management_Server..fxugme
Entity SIC Name: cn=cp_mgmt,o=QOS-Management..dn
example: CN=cp_mgmt,O=US_Management_Server..fxugme

Here the index file is selected as default. The name of default index file is "main".

If you have not changed the index setting then most certainly your default index setting would be 'main'.



splunk>
App: Check Point Analytics App by QOS
Administrator
Messages
Settings
Activity
Help
Find
Summary
Firewall
Application Control and URL Filtering
IPS
Alerts
Help
Check Point Analytics App by QOS
Edit
More Info
Total Packets dropped by Firewall
1
+28%
Connections blocked by Application Control blade
N/A
Number of reporting firewalls
Number of firewall
2
Internal Unique Source IP Addresses
274
+953%
External Unique Source IP Addresses
43645
+79%

Summary

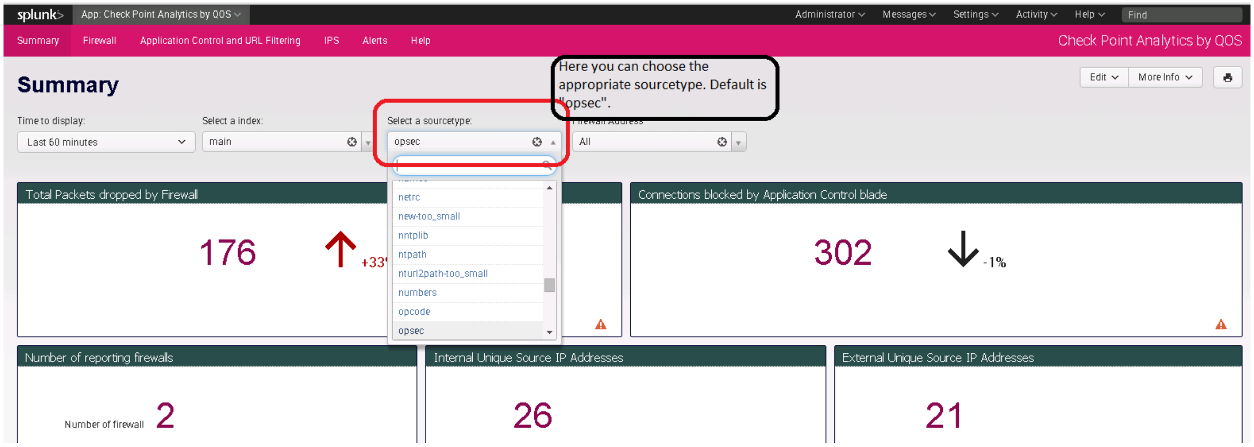
Time to display: Last 60 minutes
Select a index: index_prog
history
index_prog
main
summary
Select a sourcetype: opsec
Firewall Address: All

Use this drop down to select appropriate index file which stored Check Point logs. Default is "main".

Select a sourcetype:

Every data which is indexed by Splunk will be associated with some sourcetype. By default the sourcetype created by Check Point LEA app is **opsec**.

You can choose appropriate sourcetype from the dropdown list as per your setting. If you are not sure keep the default value.

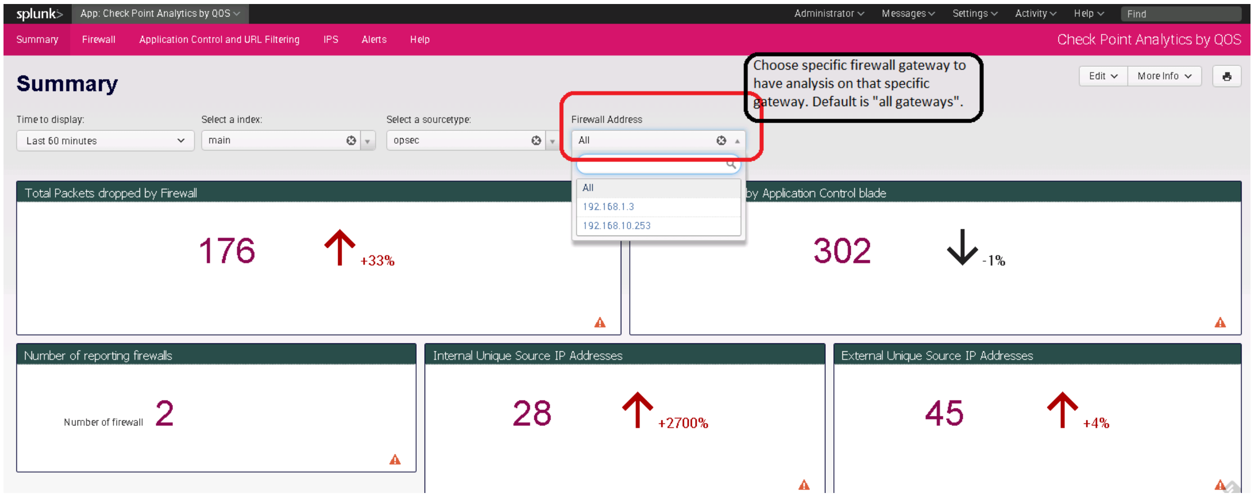

splunk>
App: Check Point Analytics by QOS
Administrator
Messages
Settings
Activity
Help
Find
Summary
Firewall
Application Control and URL Filtering
IPS
Alerts
Help
Check Point Analytics by QOS
Edit
More Info
Summary
netrc
new-too_small
nntplib
ntpath
nturl2path-too_small
numbers
opcode
opsec
Total Packets dropped by Firewall
176
+33
Connections blocked by Application Control blade
302
-1%
Number of reporting firewalls
Number of firewall
2
Internal Unique Source IP Addresses
26
External Unique Source IP Addresses
21

Here you can choose the appropriate sourcetype. Default is "opsec".

Time to display: Last 60 minutes
Select a index: main
Select a sourcetype: opsec
Firewall Address: All

Firewall Address:

If your organization is having multiple Check Point gateways and if you want analytics for specific Gateway then you can choose the appropriate gateway from the list. By default all the logs generated by these gateways will be selected.


splunk>
App: Check Point Analytics by QOS
Administrator
Messages
Settings
Activity
Help
Find
Summary
Firewall
Application Control and URL Filtering
IPS
Alerts
Help
Check Point Analytics by QOS
Edit
More Info
Summary
All
192.168.1.3
192.168.10.253
Total Packets dropped by Firewall
176
+33%
by Application Control blade
302
-1%
Number of reporting firewalls
Number of firewall
2
Internal Unique Source IP Addresses
28
+2700%
External Unique Source IP Addresses
45
+4%

Choose specific firewall gateway to have analysis on that specific gateway. Default is "all gateways".

Time to display: Last 60 minutes
Select a index: main
Select a sourcetype: opsec
Firewall Address: All

SUMMARY

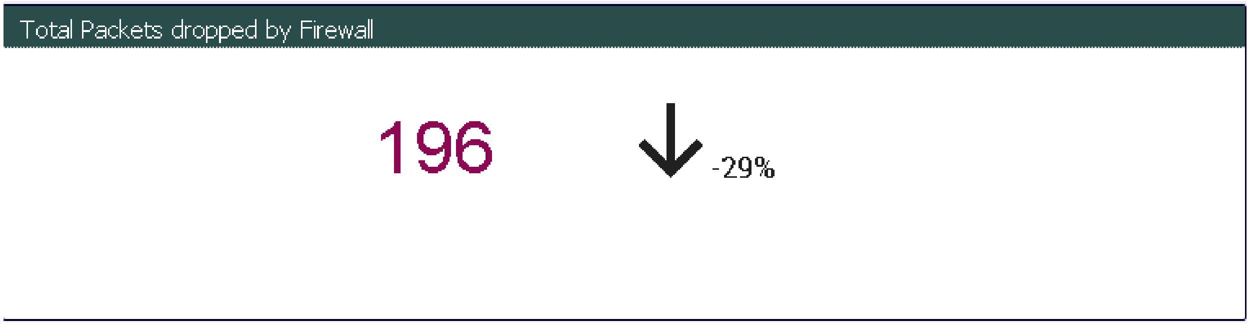
Total Packets dropped by Firewall.

This windows will display the number of connections dropped by Check Point's Firewall blade. Essentially a very high number or significant growth % in dropped value indicates lots of packets hitting clean up rule or any other drop rule.

You will also notice an arrow which will show if the dropped connections were less/more compared to last period.

For example if your setting for Time to Display is default (60 mins) and you ran this app at 3:38PM then upward arrow means that as compared to connection drop between 1:38PM - 2:38PM the connection drop between

2:38PM - 3:38PM has gone up.


Total Packets dropped by Firewall

196 ↓ -29%

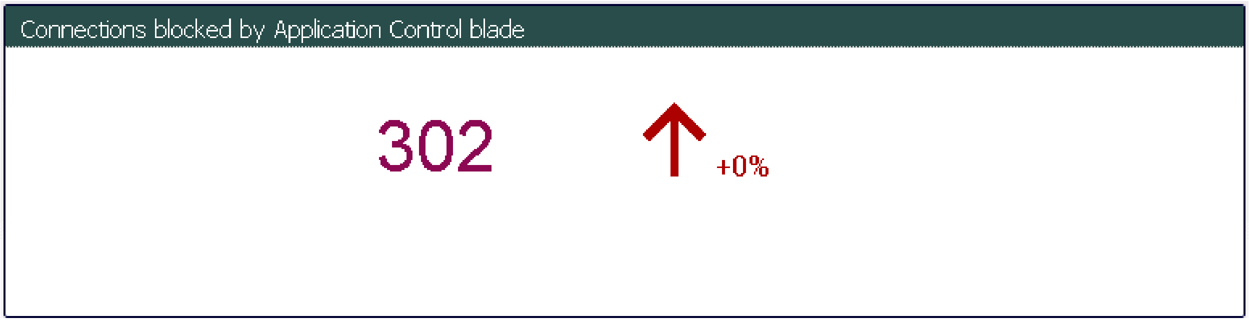
Connections blocked by Application Control blade

This windows will display the number of connections dropped by Check Point's Application and URL Filtering blade. Essentially a very high number or significant growth % in dropped value indicates lots of connections are getting dropped by App and URL Filtering block rule.

You will also notice an arrow which will show if the dropped connections were less/more compared to last period.

For example if your setting for Time to Display is default (60 mins) and you ran this app at 3:38PM then upward arrow means that as compared to connection drop between 1:38PM - 2:38PM the connection drop between

2:38PM - 3:38PM has gone up.

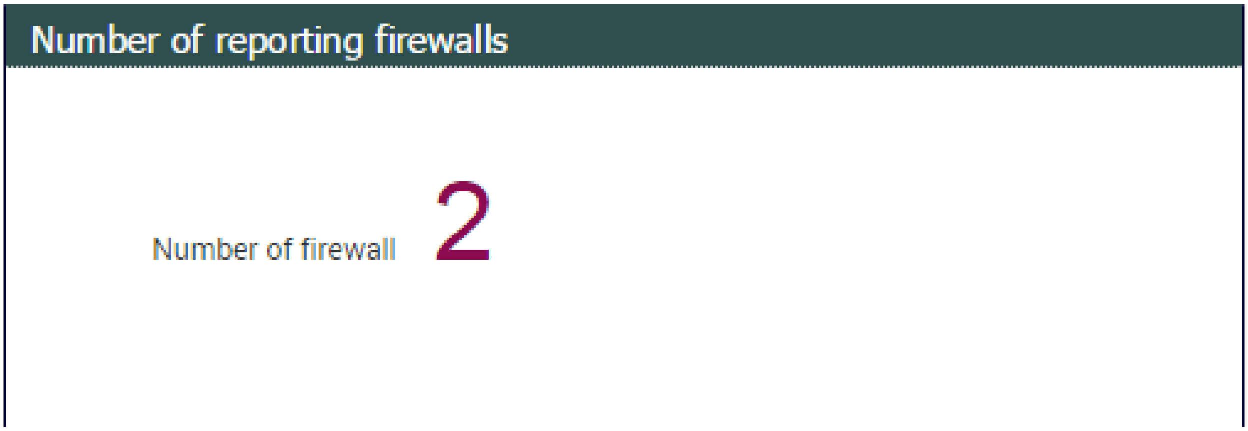


Number of reporting firewalls

This window displays the number of Check Point gateways sending log to Management Server/Log Server. Please note that logs generated by Management Server will also be counted as distinct gateway.

So ideally you should at least notice 2 Firewall gateways. As most of the Management Server logs are control messages related to licensing, disk utilization etc it will not hamper any other result anywhere in this App.

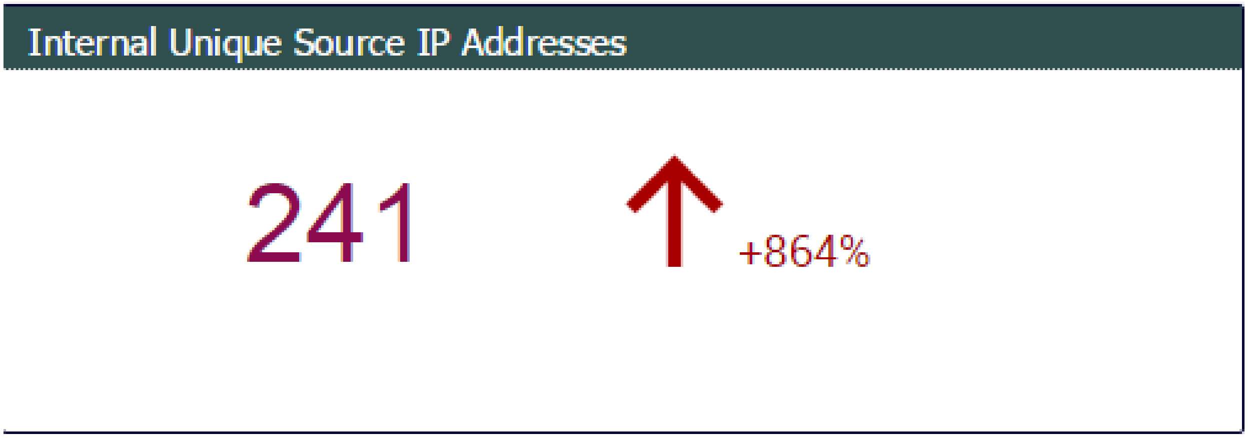
If you want to analyze logs of specific gateway then please select the appropriate Firewall Address from the dropdown list.



Internal Unique Source IP Addresses

You will get the total number of unique local IP address which are behind your firewall. It is assumed that your local address in the range 10.0.0.0/8, 172.16.0.0/12 & 192.168.0.0/16 [RFC 1918].

As sudden increase in Internal Unique IP addresses means a rouge machine or virus infected desktop/server.

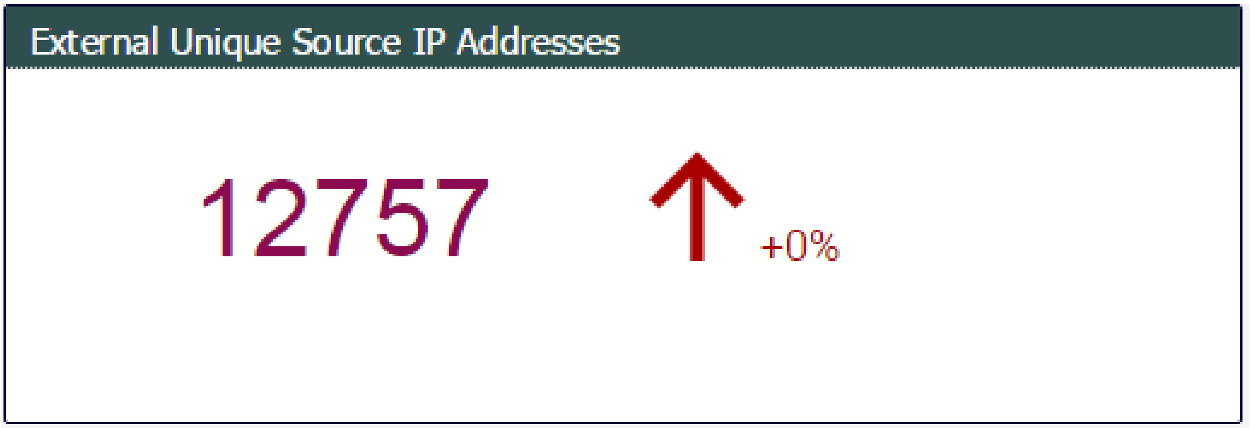


Internal Unique Source IP Addresses

241 ↑ +864%

External Unique Source IP Addresses

This window will give total number of unique external IP addresses who are trying to access your servers hosted behind Check Point Firewall.

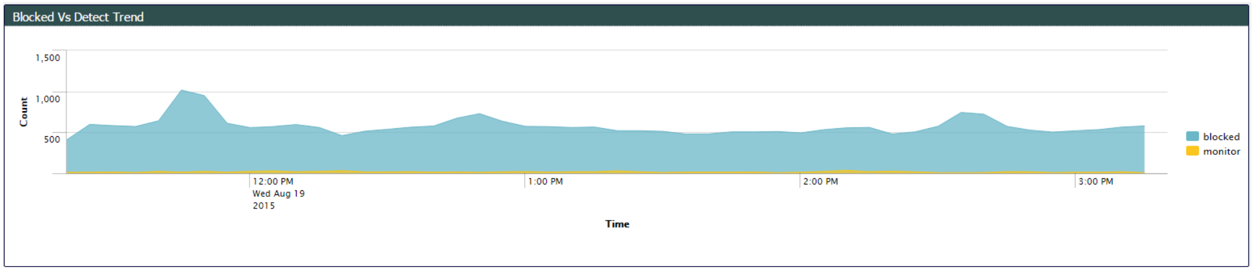


External Unique Source IP Addresses

12757 ↑ +0%

Blocked Vs Detect Trend

Check Point IPS settings allow you to set certain signatures in Prevent or in Detect mode. This window will show a trend between Prevent and Detect mode as per the your Time to Display setting.

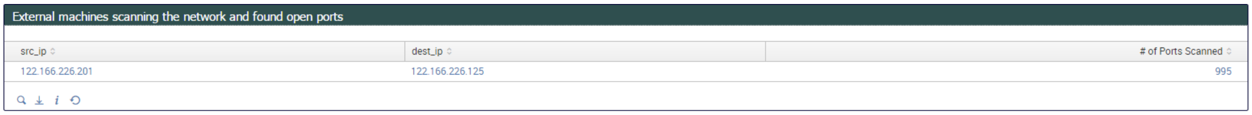


Last received 5 critical cluster info

In this window you will notice any logs generated by Check Point clusterXL feature. Most of the times we have noticed that production clusterXL failover for some reason or the other. This window will provide details about such issues with clusterXL.

External machines scanning the network and found open ports

You will see a list of external IP addresses which are scanning your network. You can block them in your firewall rulebase or IPS geo protection setting of Check Point.



External machines scanning the network and found open ports

src_ip	dest_ip	# of Ports Scanned
122.166.226.201	122.166.226.125	995

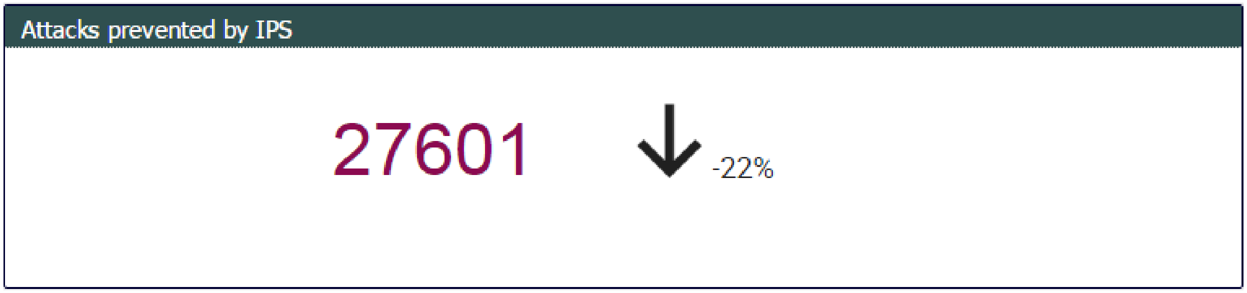
Attacks prevented by IPS

Suppose some IPS signatures are configured in Prevent mode. Then this number will show how many attacks were prevented by Check Point IPS in specified time.

You will also notice an arrow which will show if the attacks were less/more compared to last period.

For example if your setting for Time to Display is default (60 mins) and you ran this app at 00:40AM then downward arrow means that as compared to attacks between 10:40PM - 11:40PM the attacks between

11:40PM - 00:40AM has gone down.



Attacks prevented by IPS

27601 ↓ -22%

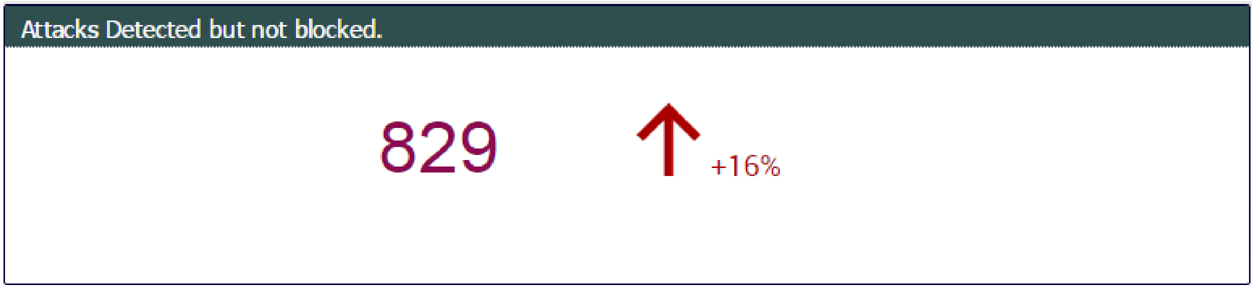
Attacks Detected but not blocked by IPS

Suppose some IPS signatures are configured in Detect mode. Then this number will show how many attacks were detected by Check Point IPS in specified time.

You will also notice an arrow which will show if the attacks were less/more compared to last period.

For example if your setting for Time to Display is default (60 mins) and you ran this app at 3:38PM then upward arrow means that as compared to attacks between 1:38PM - 2:38PM the attacks between

2:38PM - 3:38PM has gone up.



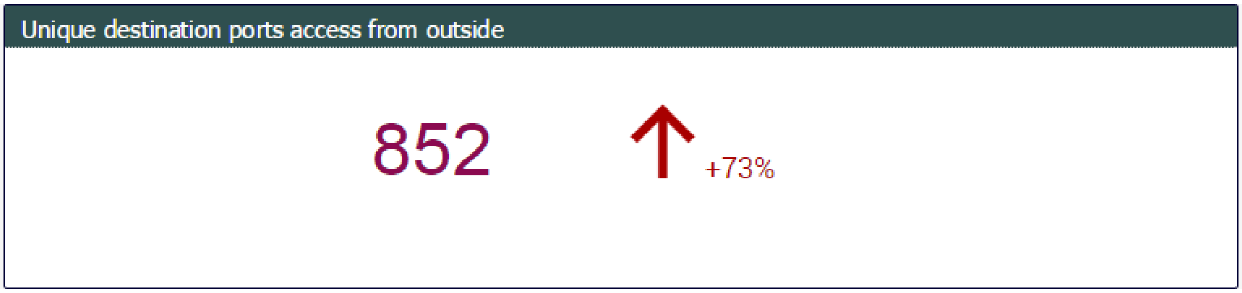
Attacks Detected but not blocked.

829 ↑ +16%

Unique destination ports access from outside

Number of unique ports being accessed from internet. These ports could be either blocked or allowed as per your firewall rulebase.

If you have few web servers, mail server and some other servers ideally you should see only very few ports getting accessed from internet. A very high number means someone trying to scan your network and that could lead to possible threat. Screen shot below shows that a very high unique ports being accessed from Internet. If your firewall rulebase is in good shape you need not worry much but if you have porous rulebase you should take immediate action.



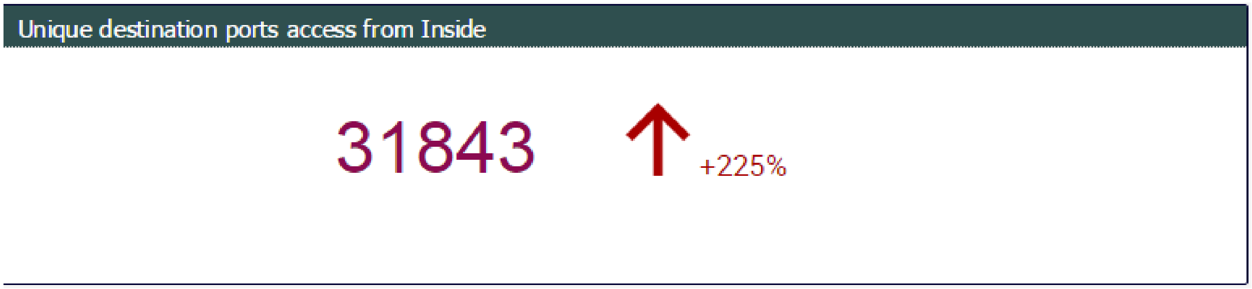
Unique destination ports access from outside

852 ↑ +73%

Unique destination ports access from Inside

Number of unique ports being accessed from Internal Network. These ports could be either blocked or allowed as per your firewall rulebase.

Generally internal users need http, https, DNS, ftp, icmp and other few ports to be open on Firewall. A very high number indicates serious problem. This means some machines are infected by Bot or Virus or some other malware.



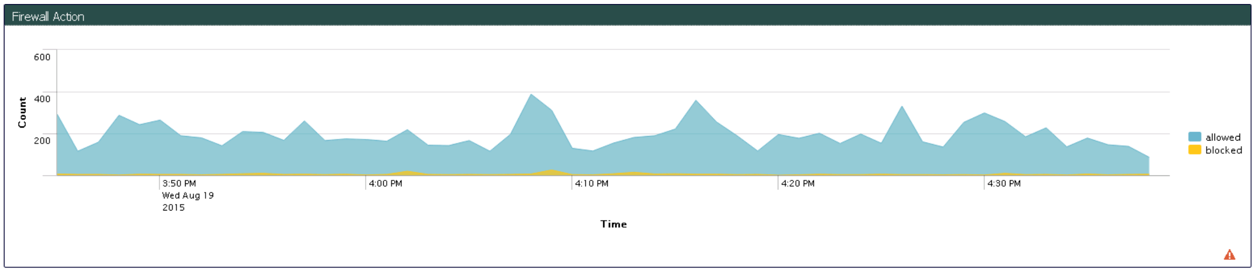
Unique destination ports access from Inside

31843 ↑ +225%

FIREWALL

Firewall Action

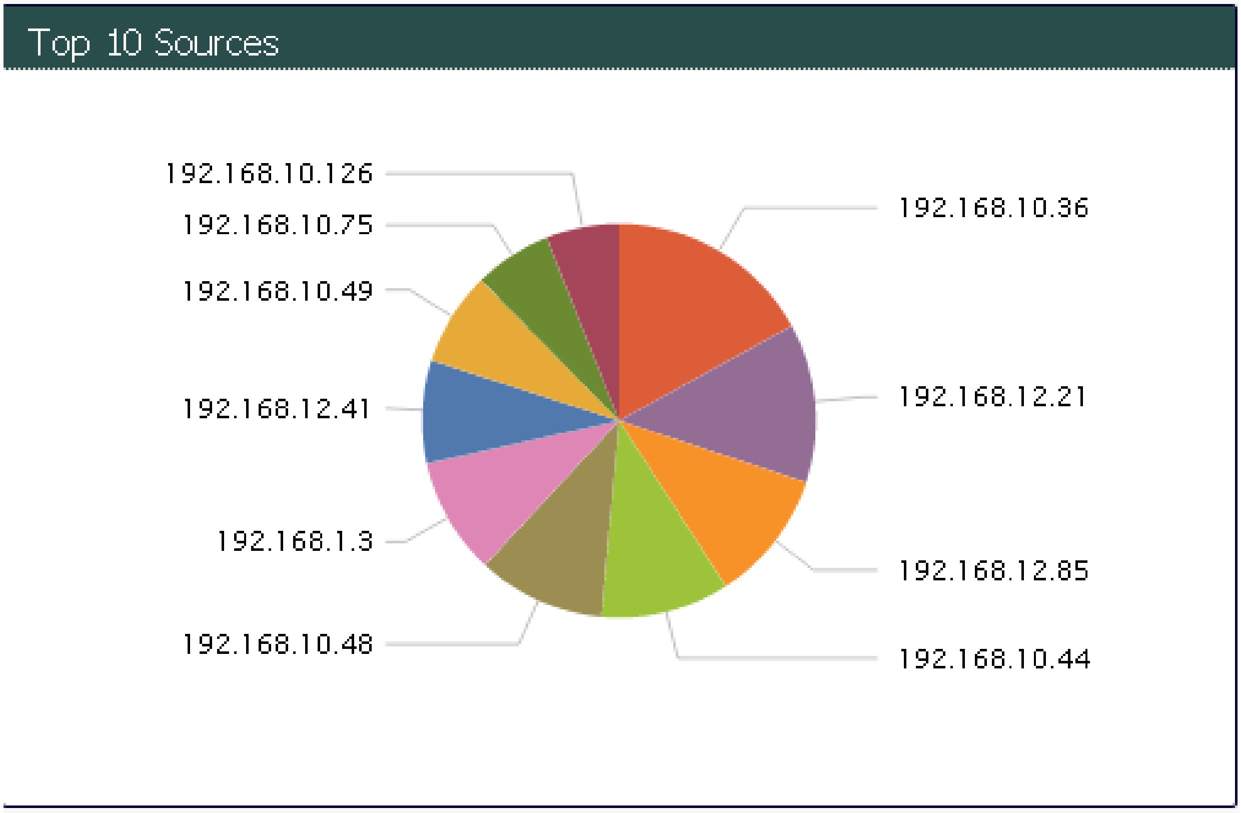
You will notice a trend between accepted and blocked packets by Check Point's firewall rulebase.



Top 10 Sources

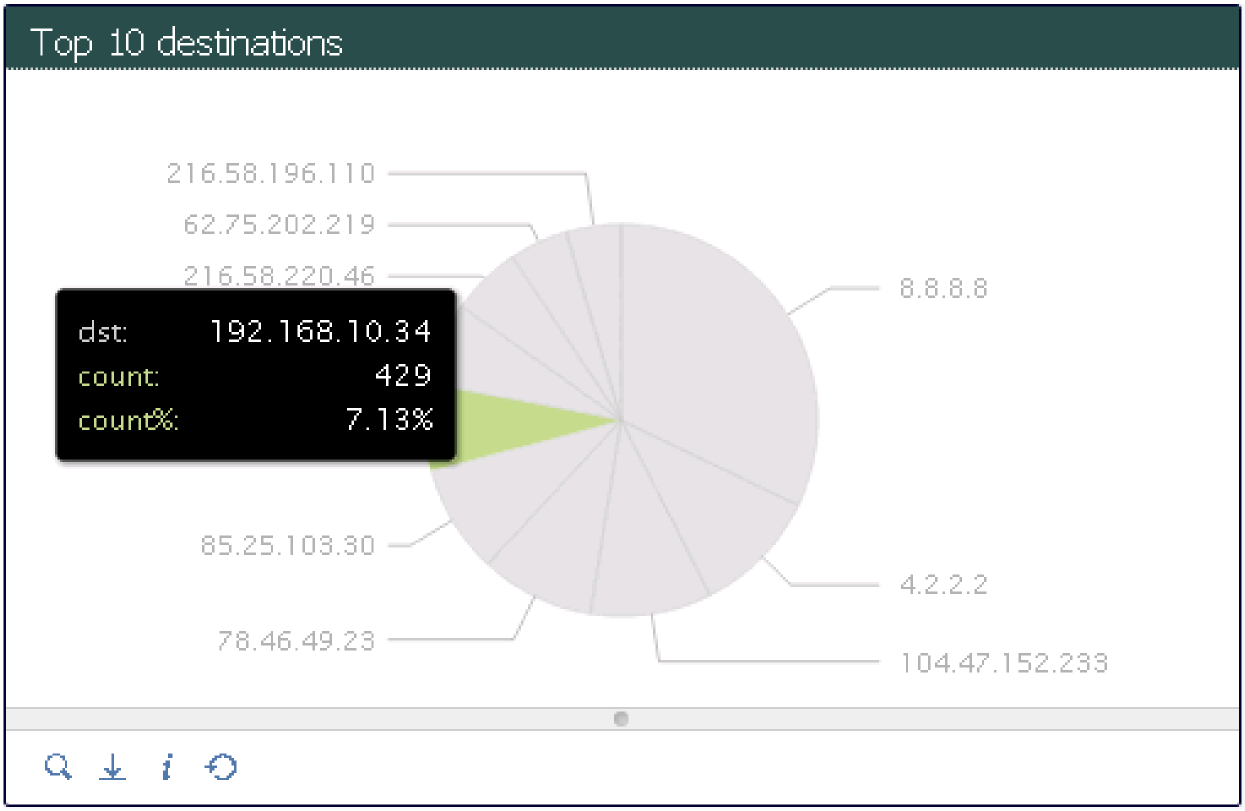
A list of top 10 local machines. This list is created based on amount of Check Point logs some machines generate. This window ignores icmp packets and only considers allowed traffic.

It is assumed that your local address in the range 10.0.0.0/8, 172.16.0.0/12 & 192.168.0.0/16 [RFC 1918].



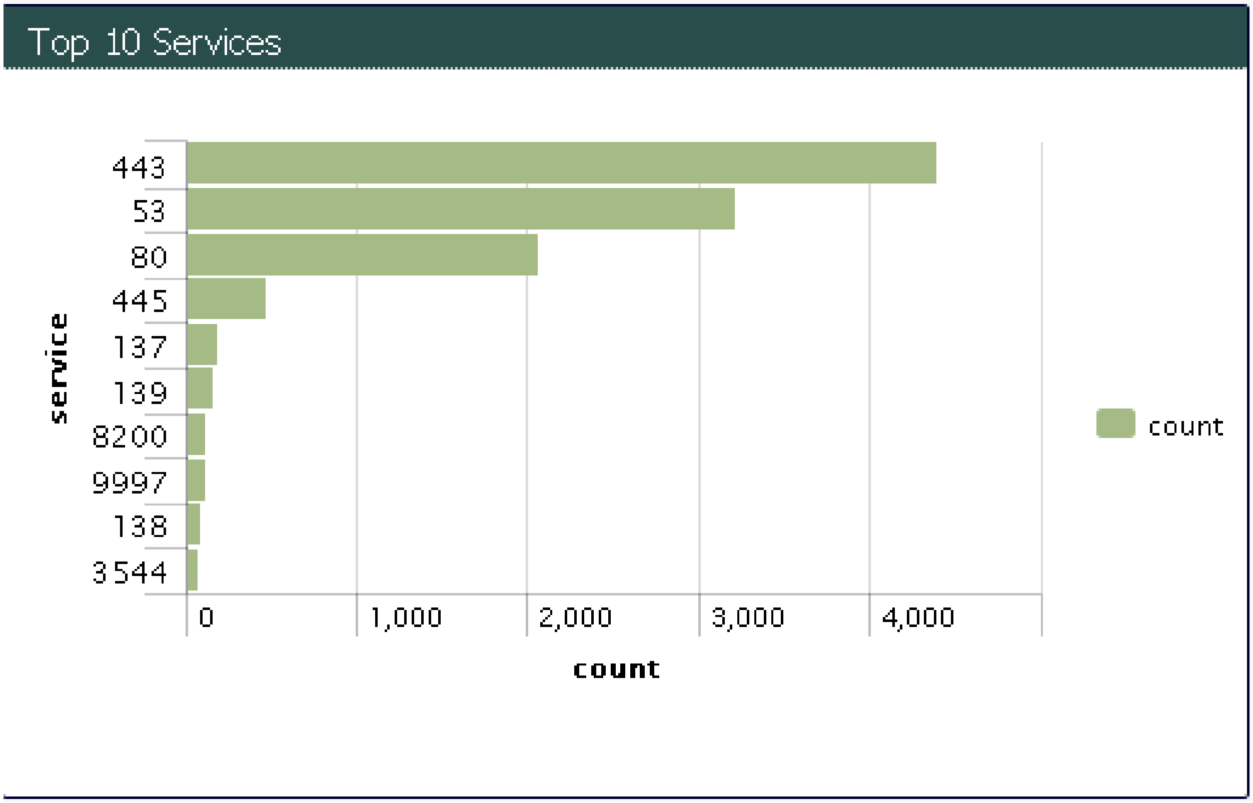
Top 10 destinations

A list of top 10 destination IP addresses. You will know which all servers your local users are connecting. Any ip which is not from the range 10.0.0.0/8, 172.16.0.0/12 & 192.168.0.0/16 [RFC 1918] is considered external IP Address.



Top 10 Services

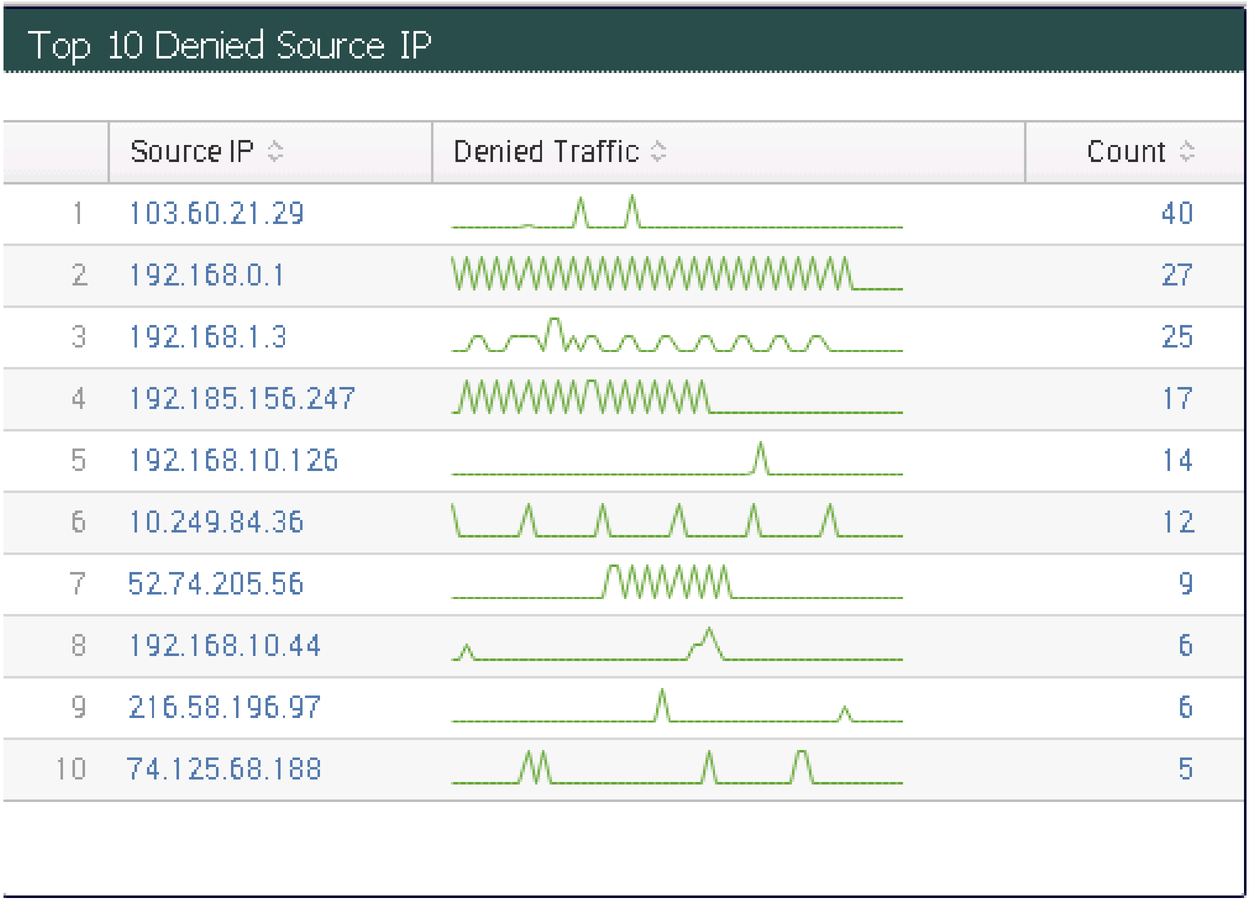
A list of services/ports your local users are trying to access. This will consider all ports being used by local user irrespective of whether those ports are allowed or dropped by Firewall.



Top 10 Denied Source IP

This window will show a trend of those IP Addresses which are blocked by Check Point gateway.

These IP Addresses could be internal or external.



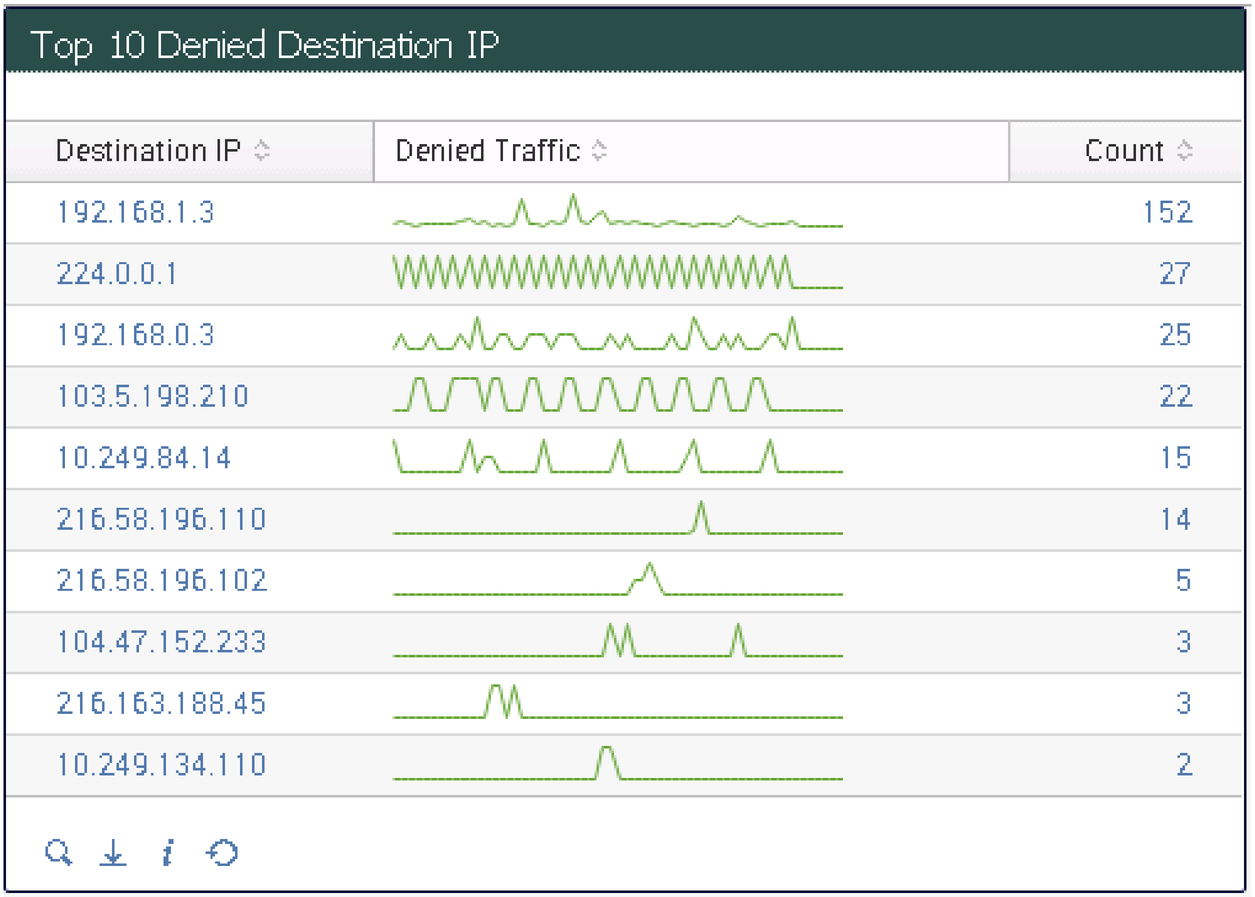
Top 10 Denied Source IP

	Source IP	Denied Traffic	Count
1	103.60.21.29		40
2	192.168.0.1		27
3	192.168.1.3		25
4	192.185.156.247		17
5	192.168.10.126		14
6	10.249.84.36		12
7	52.74.205.56		9
8	192.168.10.44		6
9	216.58.196.97		6
10	74.125.68.188		5

Top 10 Denied Destination IP

A list of top 10 destination IP Addresses which are not allowed by Check Point Gateway.

There are some internal users who are trying to access these servers which are anyway not allowed by your Firewall.

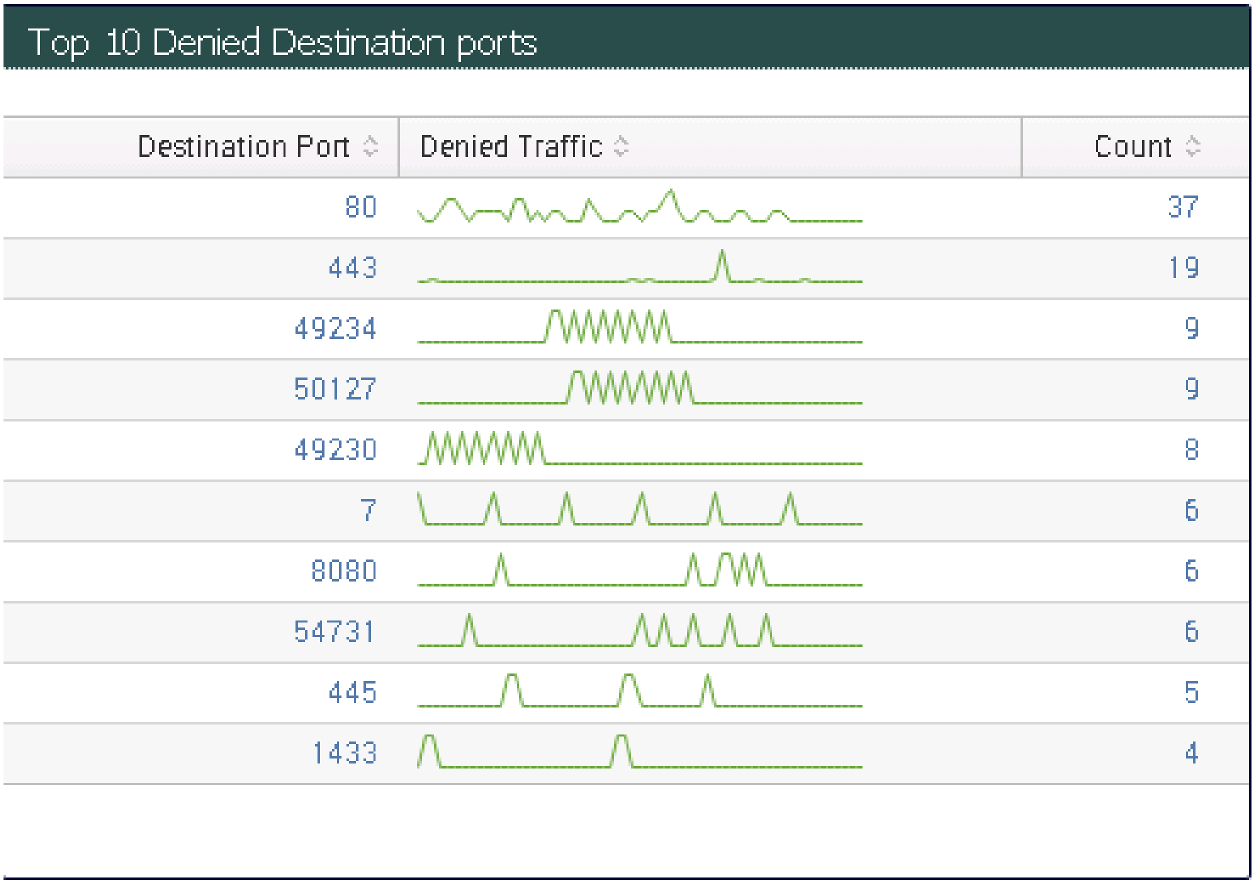


Top 10 Denied Destination IP

Destination IP	Denied Traffic	Count
192.168.1.3		152
224.0.0.1		27
192.168.0.3		25
103.5.198.210		22
10.249.84.14		15
216.58.196.110		14
216.58.196.102		5
104.47.152.233		3
216.163.188.45		3
10.249.134.110		2

Top 10 Denied Destination ports

A list of top 10 ports/services which are blocked by Check Point gateway. You will come know which all ports people are trying to access even though they are not allowed by Check Point.

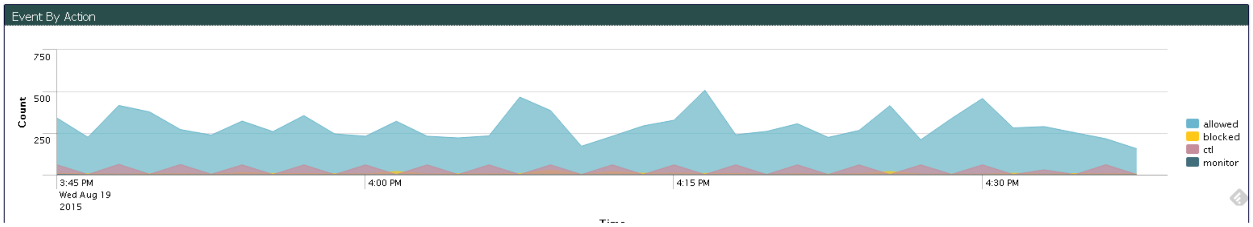


Top 10 Denied Destination ports

Destination Port	Denied Traffic	Count
80		37
443		19
49234		9
50127		9
49230		8
7		6
8080		6
54731		6
445		5
1433		4

Event By Action

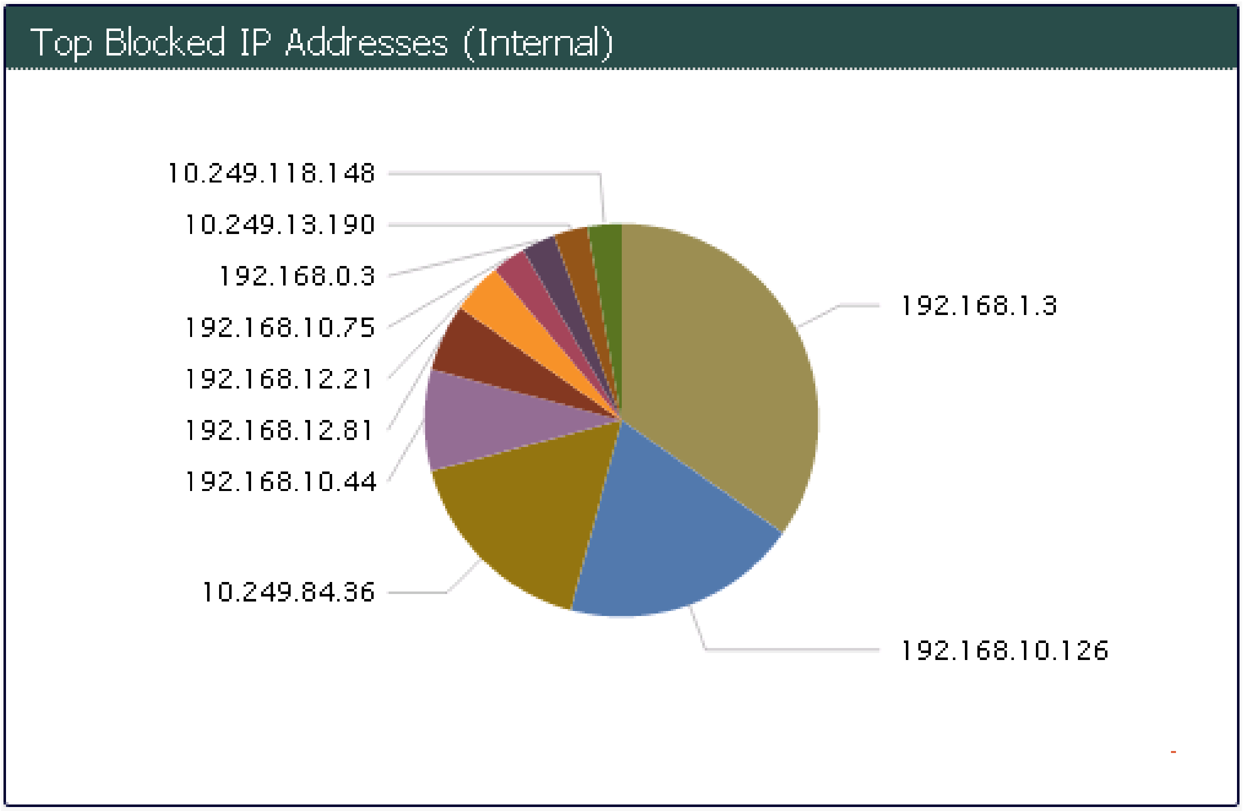
This window will display a trend of all actions taken by Check Point gateway for all security blades.



Top Blocked IP Addresses (Internal)

A list of top 10 internal IP Addresses which are blocked by Check Point gateway.

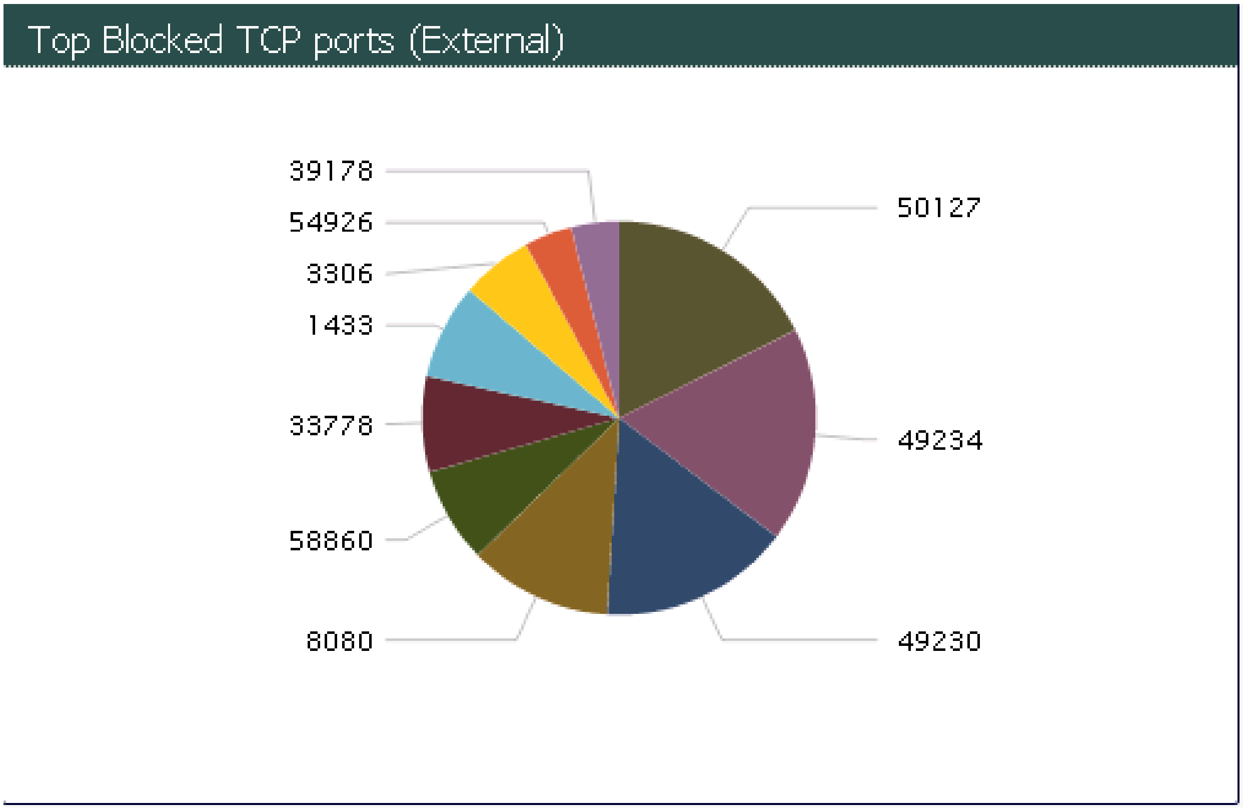
It is assumed that your local address is in the range 10.0.0.0/8, 172.16.0.0/12 & 192.168.0.0/16 [RFC 1918].



Top Blocked TCP ports (External)

A list of top 10 TCP ports/service which are blocked by Check Point gateway when these ports are accessed from Internet/external network.

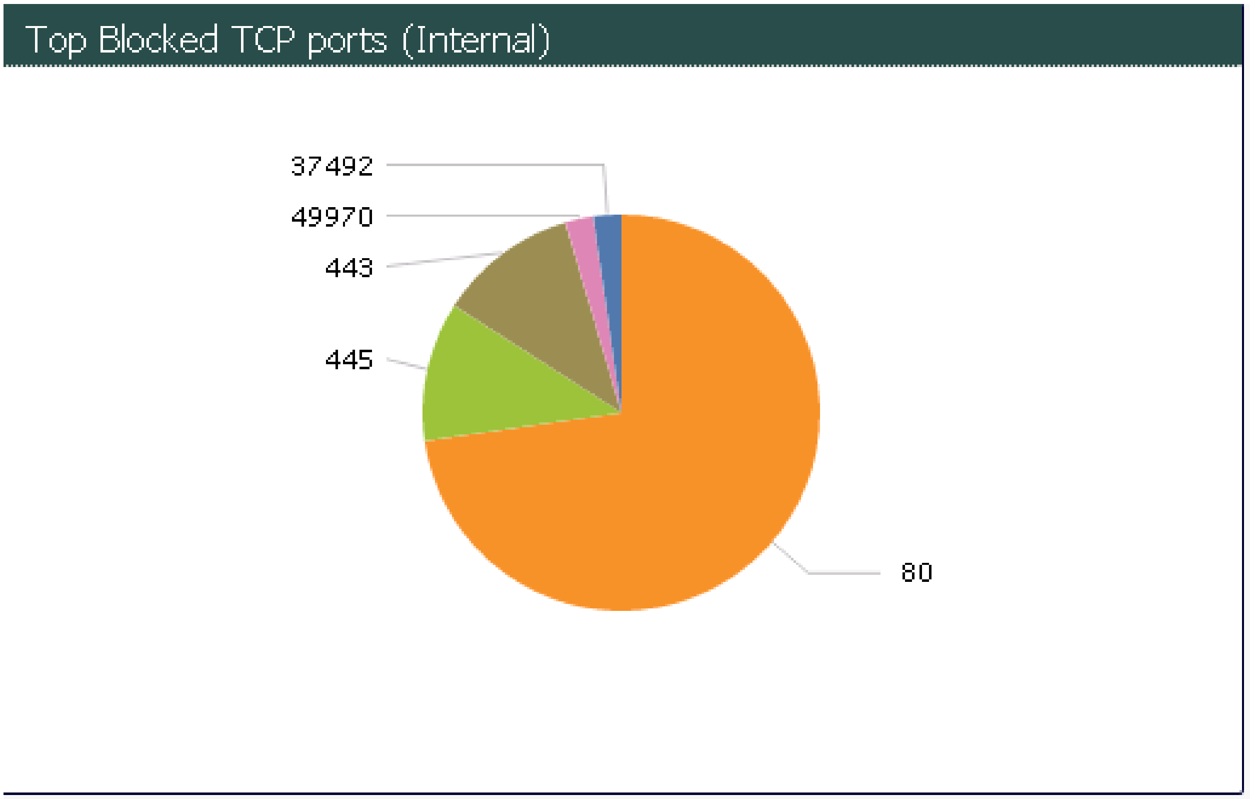
Any ip which is not from the range 10.0.0.0/8, 172.16.0.0/12 & 192.168.0.0/16 [RFC 1918] is considered external IP Address.



Top Blocked TCP ports (Internal)

A list of TCP ports/services which are blocked by Check Point gateway when accessed by local/internal users.

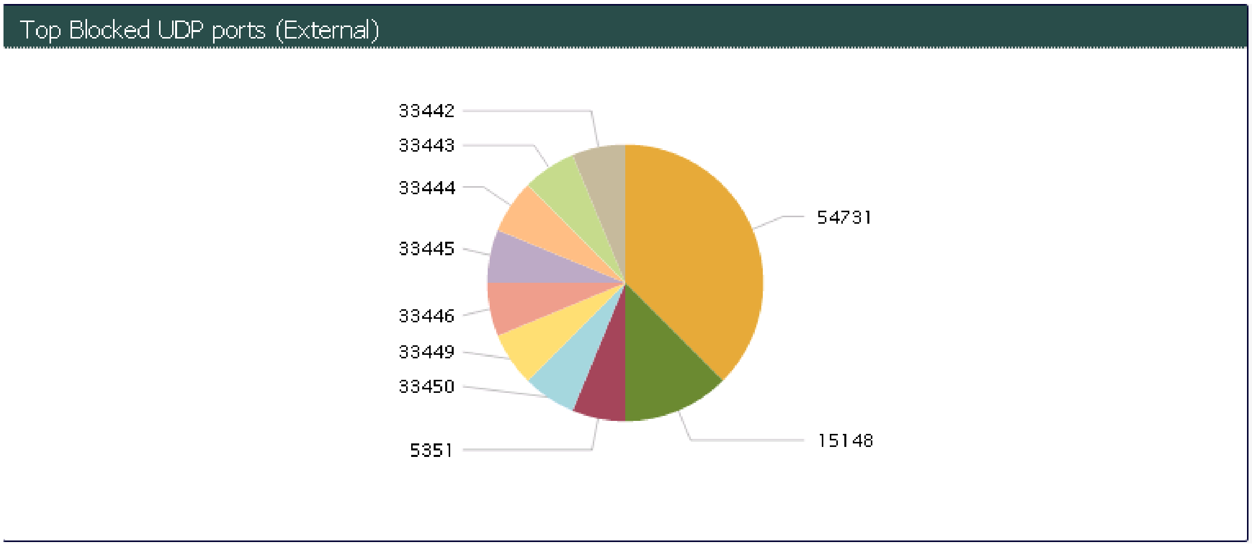
It is assumed that your local address is in the range 10.0.0.0/8, 172.16.0.0/12 & 192.168.0.0/16 [RFC 1918].



Top Blocked UDP ports (External)

A list of top 10 UDP ports/service which are blocked by Check Point gateway when these ports are accessed from Internet/external network.

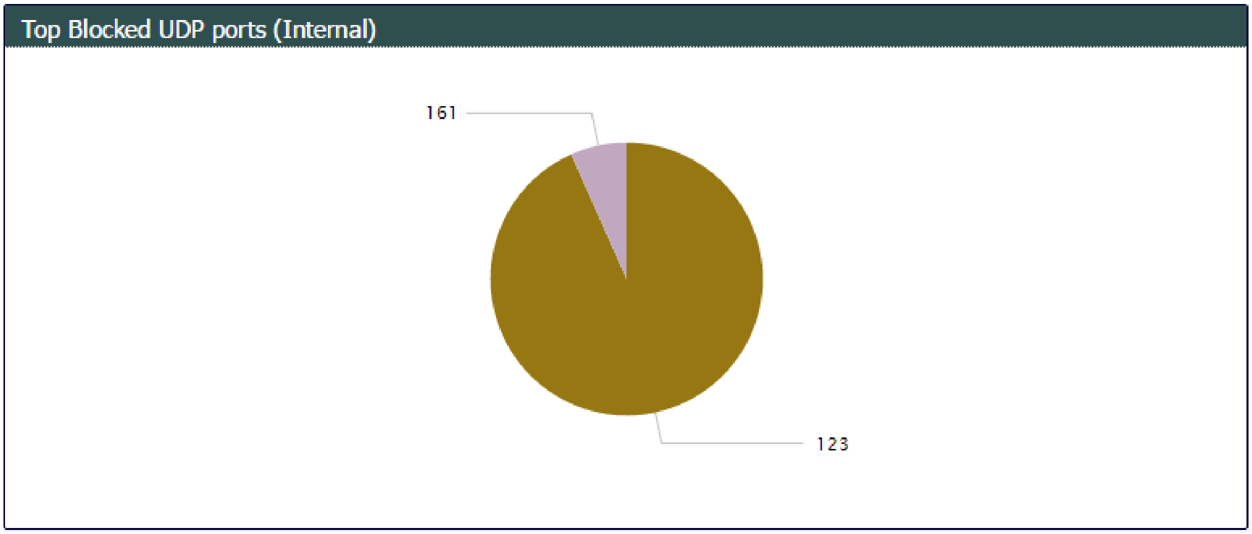
Any ip which is not from the range 10.0.0.0/8, 172.16.0.0/12 & 192.168.0.0/16 [RFC 1918] is considered external IP Address.



Top Blocked UDP ports (Internal)

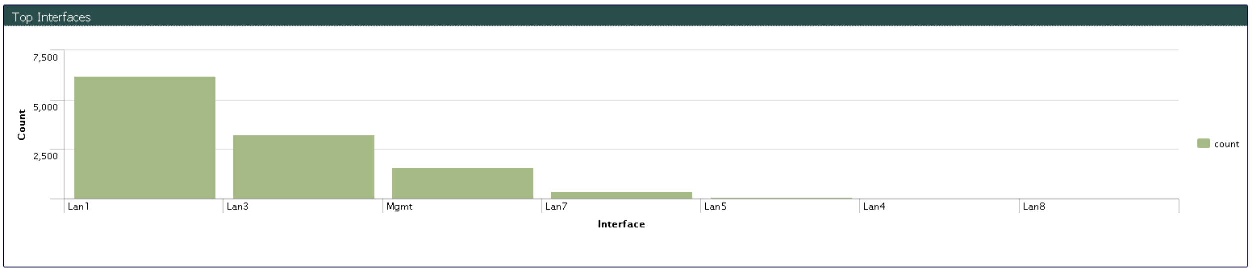
A list of UDP ports/services which are blocked by Check Point gateway when accessed by local/internal users.

It is assumed that your local address is in the range 10.0.0.0/8, 172.16.0.0/12 & 192.168.0.0/16 [RFC 1918].



Top Interfaces

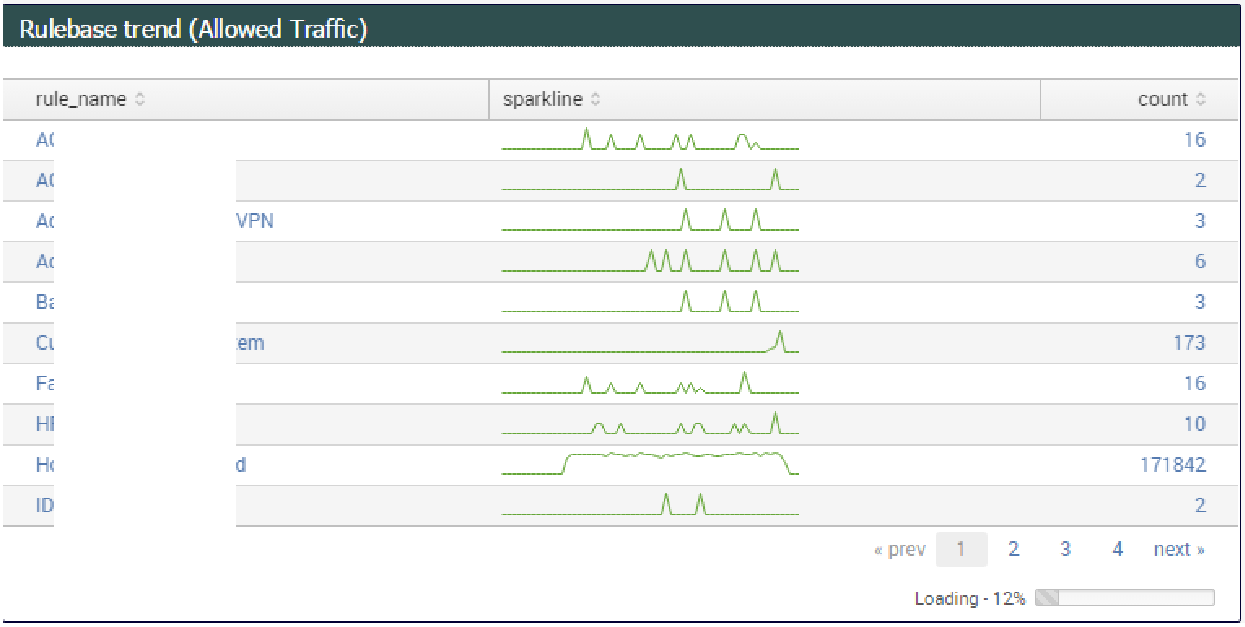
A bar chart which displays which Check Point gateway's interfaces are utilized most.



Rulebase trend (Allowed Traffic)

One can provide rule name while configuring firewall rulebase in Check Point. This window will show trend for highly utilized accepted rules. Information from this window can be used for

performance optimization.



Rulebase trend (Allowed Traffic)

rule_name	sparkline	count
A(		16
A(		2
Ac VPN		3
Ac		6
Ba		3
Cu em		173
Fa		16
HI		10
Hc d		171842
ID		2

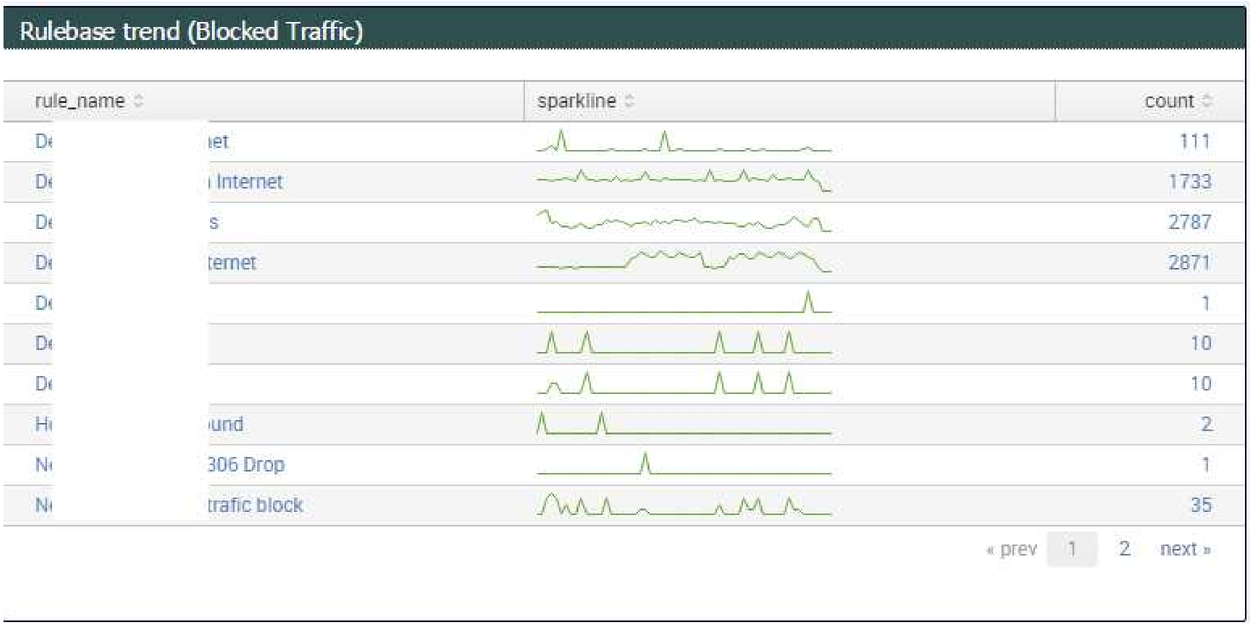
« prev 1 2 3 4 next »

Loading - 12%

Rulebase trend (Blocked Traffic)

One can provide rule name while configuring firewall rulebase in Check Point. This window will show trend for highly utilized rulebases where the connections are dropped by Check Point gateway.

Information from this window can be used for performance optimization.



Rulebase trend (Blocked Traffic)

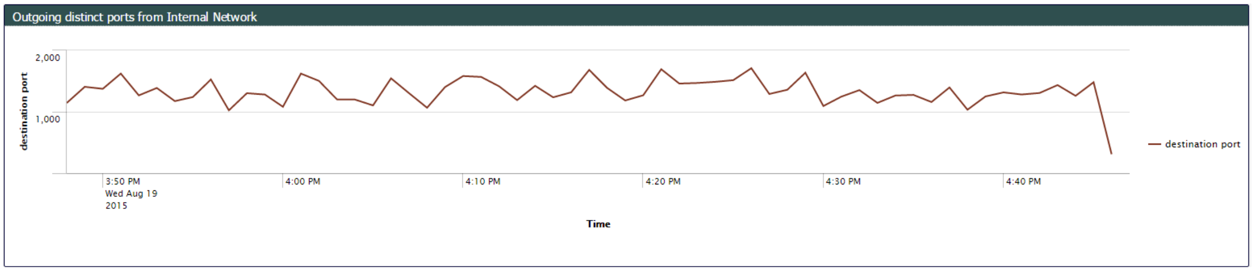
rule_name	sparkline	count
De iet		111
De Internet		1733
De s		2787
De ternet		2871
De		1
De		10
De		10
H und		2
N 306 Drop		1
N trafic block		35

« prev 1 2 next »

Outgoing distinct ports from Internal Network

This graph will demonstrate how local users are accessing the external network (internet). This graph is plotted based on unique destination ports internal users are trying access over a period of time.

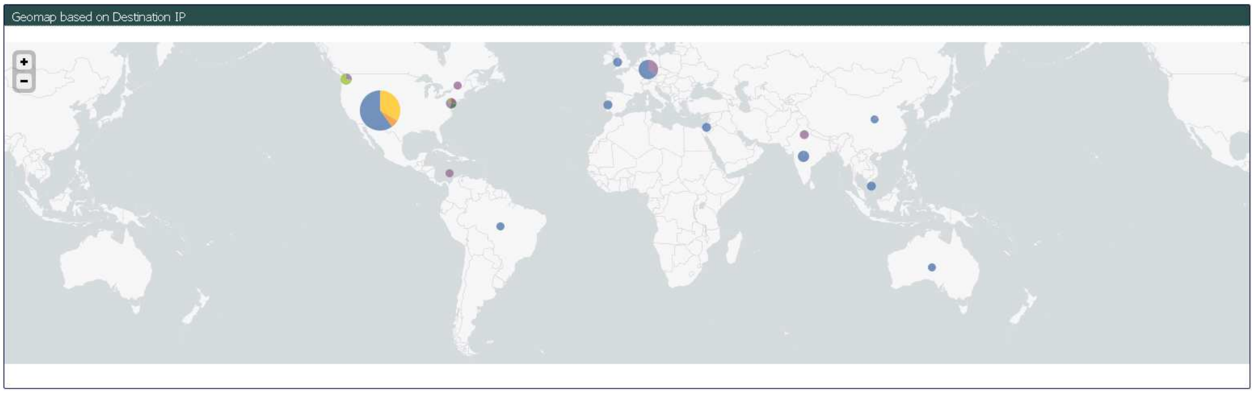
Below screenshot shows there is serious problem with internal machines. Under normal circumstances one should not see more than 100 unique ports while accessing internet. These external ports are generally common services such as DNS, http, https, ftp, smtp, icmp etc.



Geomap based on Destination IP

A world map showing which all countries internal users are connecting. Primarily these are the countries where servers are located. This map is created by using destinantion IP addresses of connection originating from

local network.

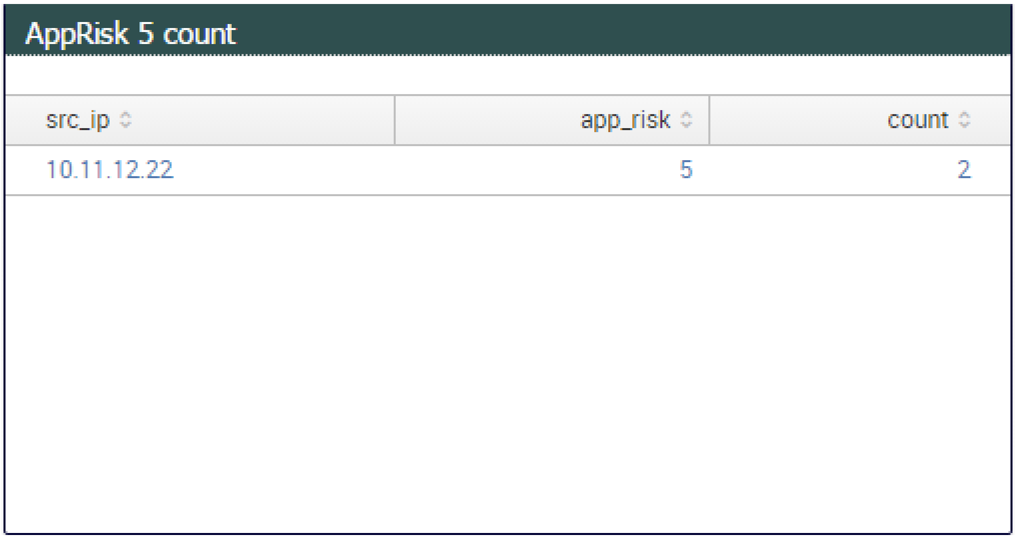


APPLICATION CONTROL AND URL FILTERING

AppRisk 5 count

A list of local IP Addresses which are trying to access high risk websites/servers. Check Point's App and URL Filtering blade has categorized millions of websites based on their risk profile.

Rating of 5 is highest rating from Check Point. You need to be careful and find out the reason why someone trying to access risky websites. Most of these websites are proxy servers and anonymizers which are used to bypass firewall.



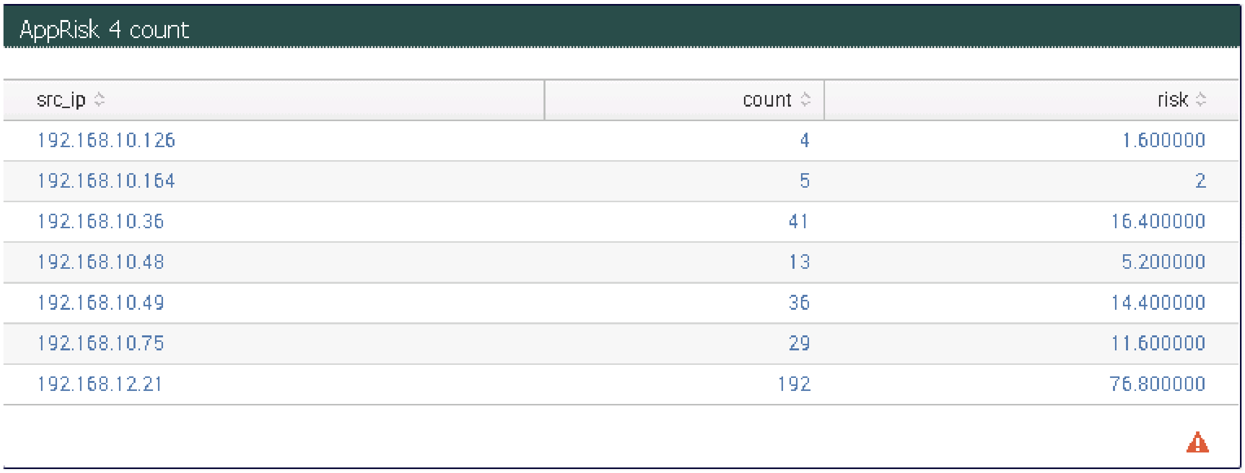
AppRisk 5 count

src_ip	app_risk	count
10.11.12.22	5	2

AppRisk 4 count

A list of local IP Addresses which are trying to access high risk websites/servers. Check Point's App and URL Filtering blade has categorized millions of websites based on their risk profile.

Rating of 4 is also considered risky by Check Point. You need to be careful and find out the reason why someone trying to access risky websites.

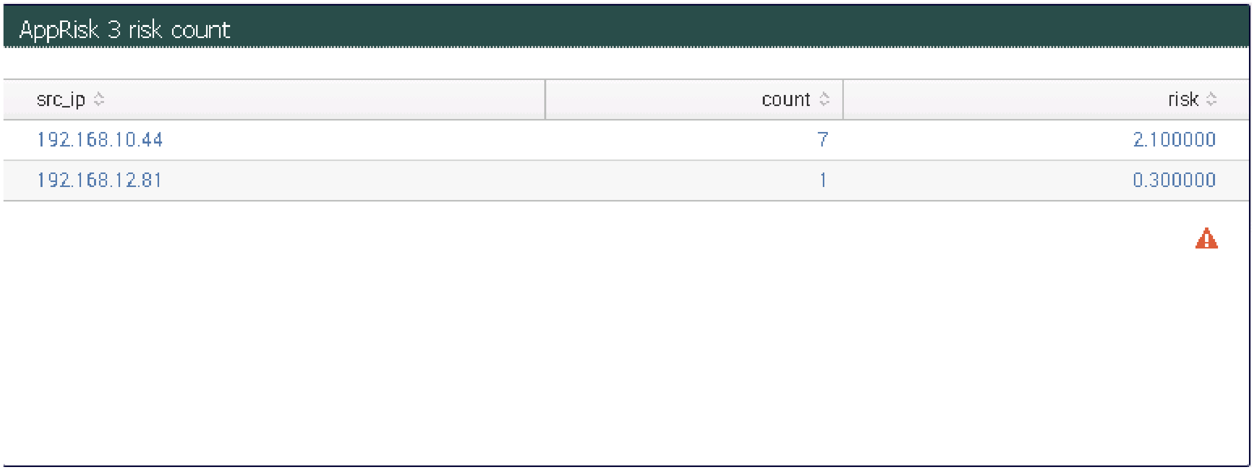


AppRisk 4 count

src_ip	count	risk
192.168.10.126	4	1.600000
192.168.10.164	5	2
192.168.10.36	41	16.400000
192.168.10.48	13	5.200000
192.168.10.49	36	14.400000
192.168.10.75	29	11.600000
192.168.12.21	192	76.800000

AppRisk 3 risk count

Same as AppRisk 4 but the risk factor is 3. The listed machines are the one trying to access risky websites which are rated as 2nd highest by Check Point.



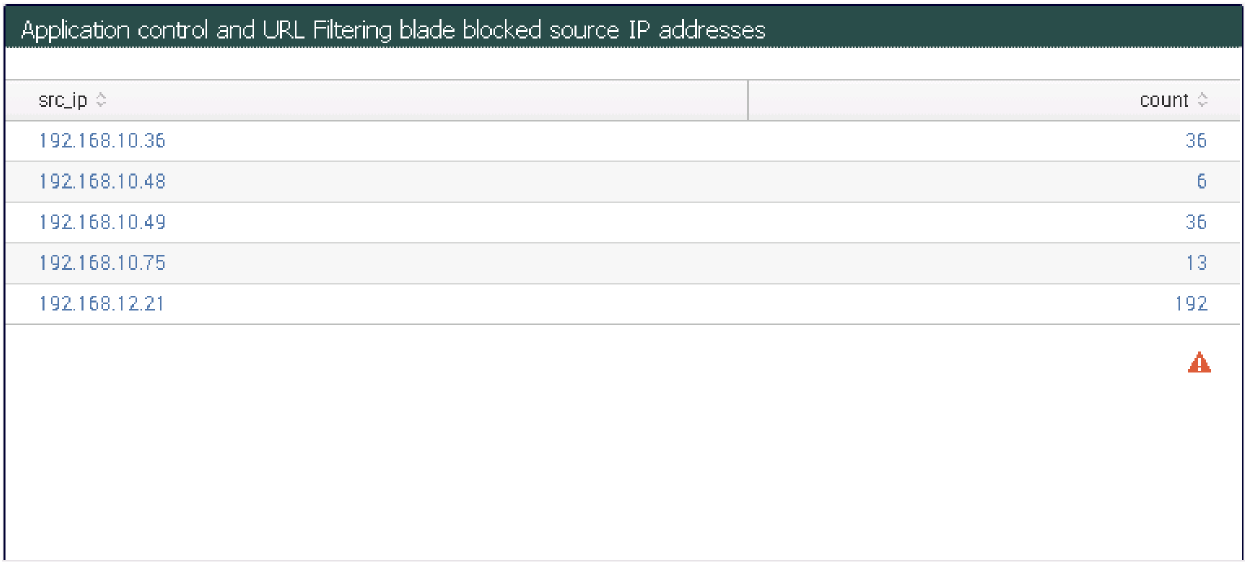
AppRisk 3 risk count

src_ip	count	risk
192.168.10.44	7	2.100000
192.168.12.81	1	0.300000

Application control and URL Filtering blade blocked source IP addresses

A list of local/internal IP Addresses which are blocked by App and URL Filtering blade of Check Point.

It is assumed that your local address is in the range 10.0.0.0/8, 172.16.0.0/12 & 192.168.0.0/16 [RFC 1918].



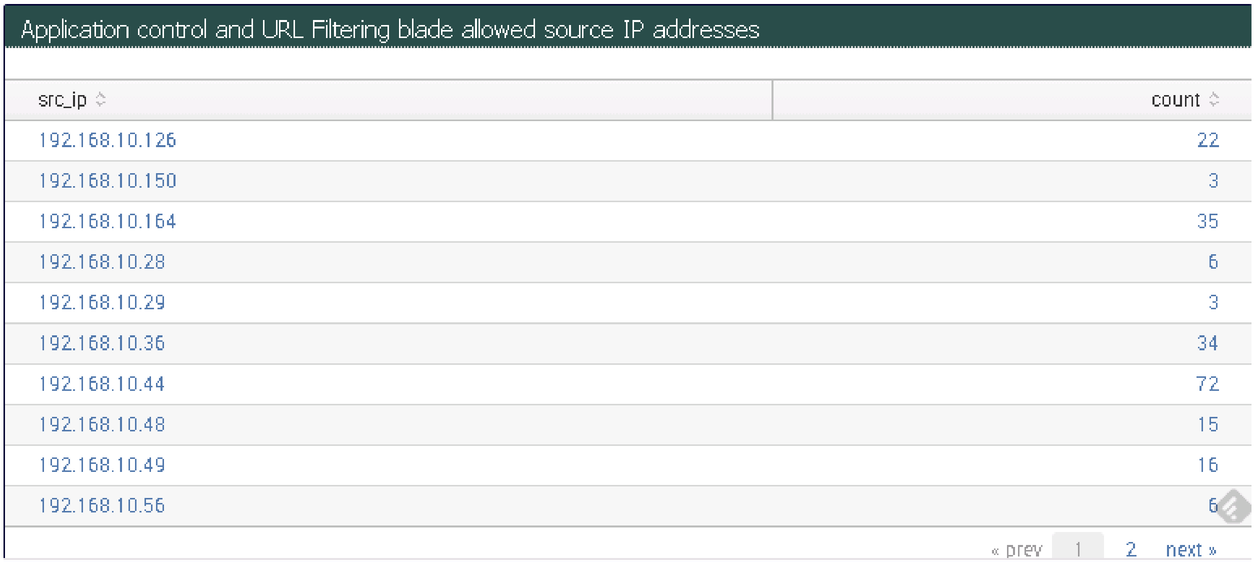
Application control and URL Filtering blade blocked source IP addresses

src_ip	count
192.168.10.36	36
192.168.10.48	6
192.168.10.49	36
192.168.10.75	13
192.168.12.21	192

Application control and URL Filtering blade allowed source IP addresses

A list of local/internal IP Addresses which are allowed by App and URL Filtering blade of Check Point.

It is assumed that your local address is in the range 10.0.0.0/8, 172.16.0.0/12 & 192.168.0.0/16 [RFC 1918].

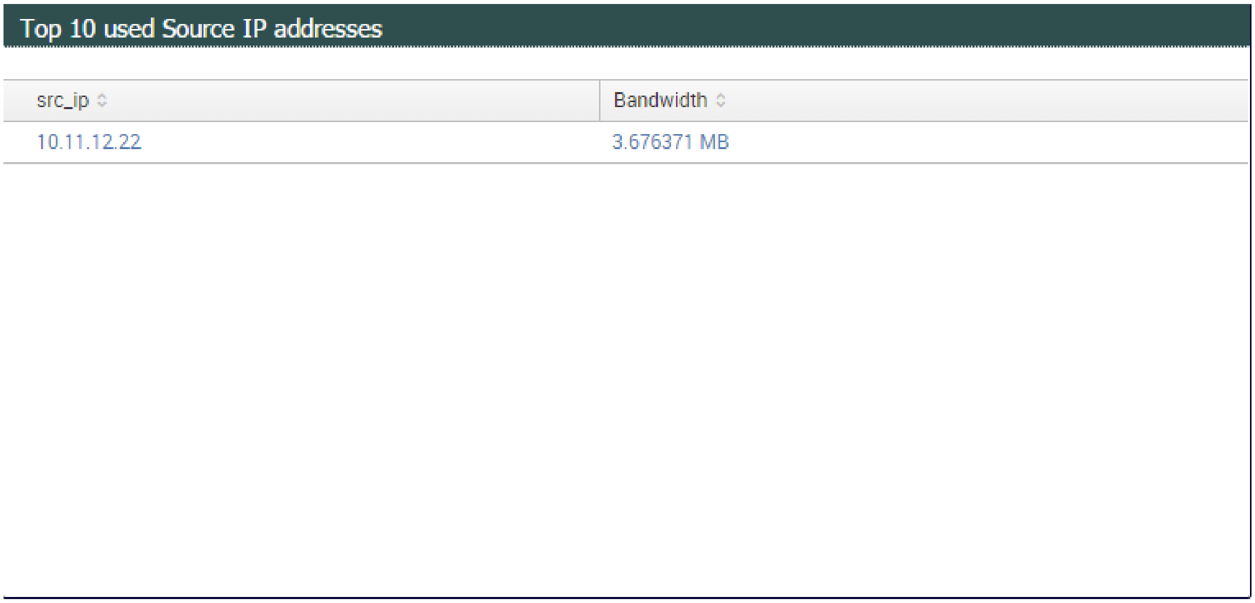


Application control and URL Filtering blade allowed source IP addresses

src_ip	count
192.168.10.126	22
192.168.10.150	3
192.168.10.164	35
192.168.10.28	6
192.168.10.29	3
192.168.10.36	34
192.168.10.44	72
192.168.10.48	15
192.168.10.49	16
192.168.10.56	6

Top 10 used Source IP addresses

A list of top 10 source ip-addresses who have been utilizing the Internet bandwidth most. You will get the IP addresses along with how much data each of these machines have downloaded. This is based on the time window you have selected.

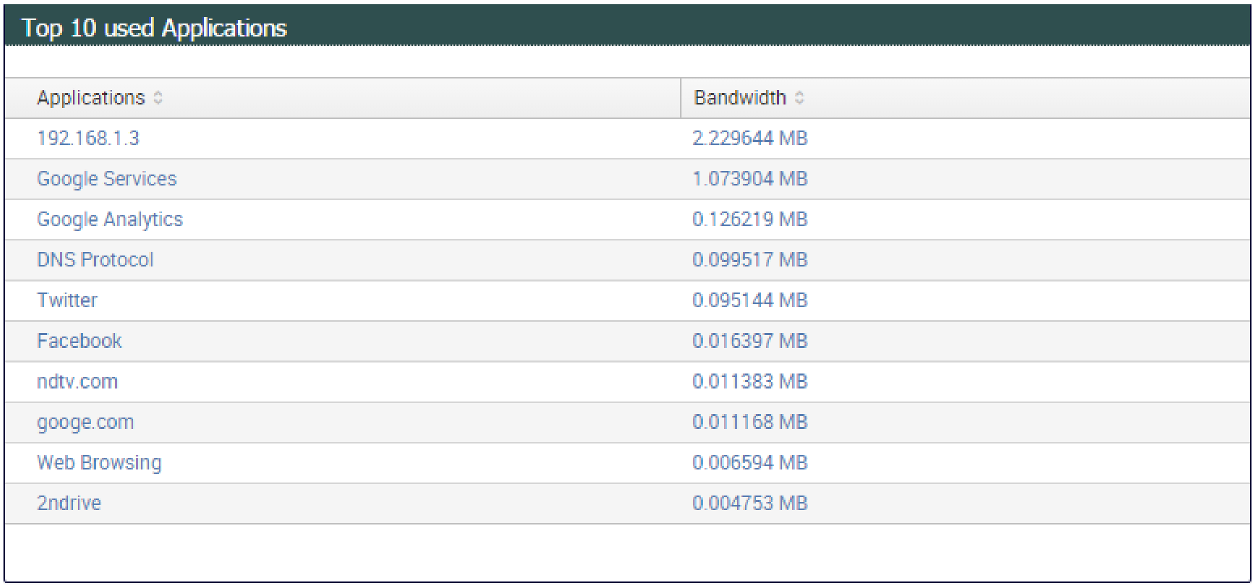


Top 10 used Source IP addresses

src_ip	Bandwidth
10.11.12.22	3.676371 MB

Top 10 used Applications

A list of top 10 applications which are used in your organization based on their bandwidth consumption.
You will get the application names along with how much data each of these applications have downloaded. This is based on the time window you have selected.

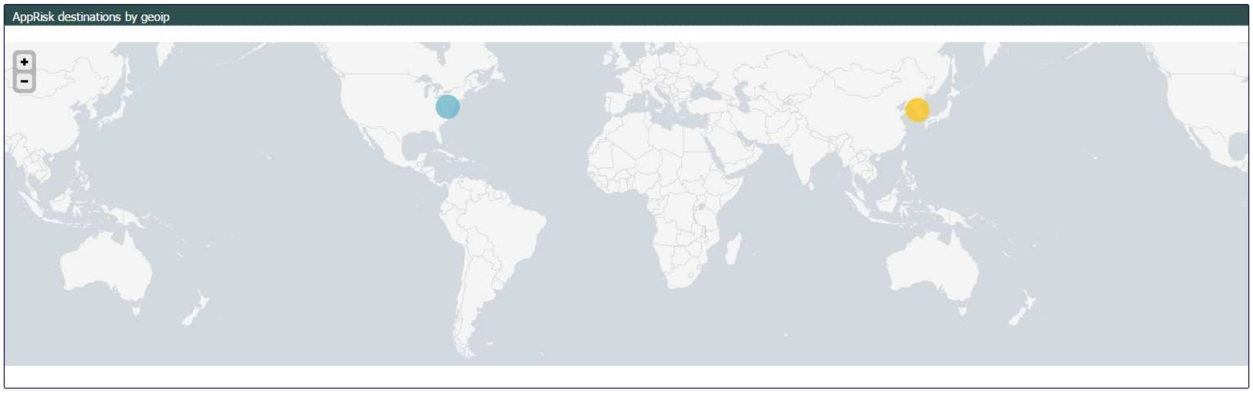


Top 10 used Applications

Applications	Bandwidth
192.168.1.3	2.229644 MB
Google Services	1.073904 MB
Google Analytics	0.126219 MB
DNS Protocol	0.099517 MB
Twitter	0.095144 MB
Facebook	0.016397 MB
ndtv.com	0.011383 MB
googe.com	0.011168 MB
Web Browsing	0.006594 MB
2ndrive	0.004753 MB

AppRisk destinations by geoip

A word map displaying where all high risk (risk score 3, 4 and 5) website located.



IPS

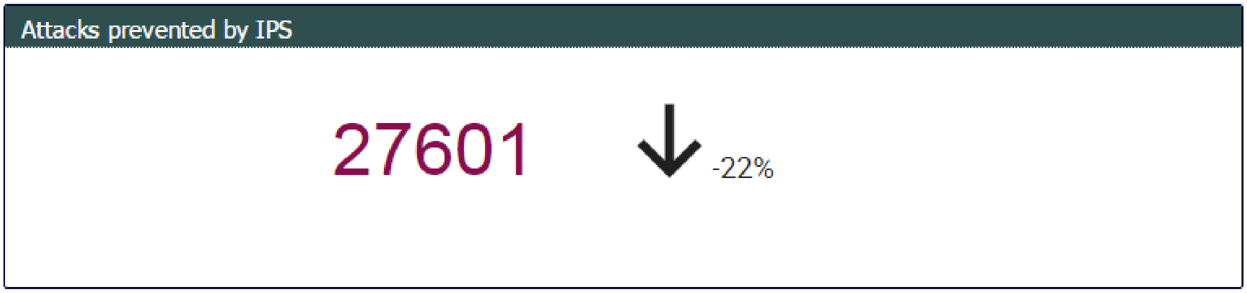
Attacks prevented by IPS

Suppose some IPS signatures are configured in Prevent mode. Then this number will show how many attacks were prevented by Check Point IPS in specified time.

You will also notice an arrow which will show if the attacks were less/more compared to last period.

For example if your setting for Time to Display is default (60 mins) and you ran this app at 00:40AM then downward arrow means that as compared to attacks between 10:40PM - 11:40PM the attacks between

11:40PM - 00:40AM has gone down.


Attacks prevented by IPS

27601 ↓ -22%

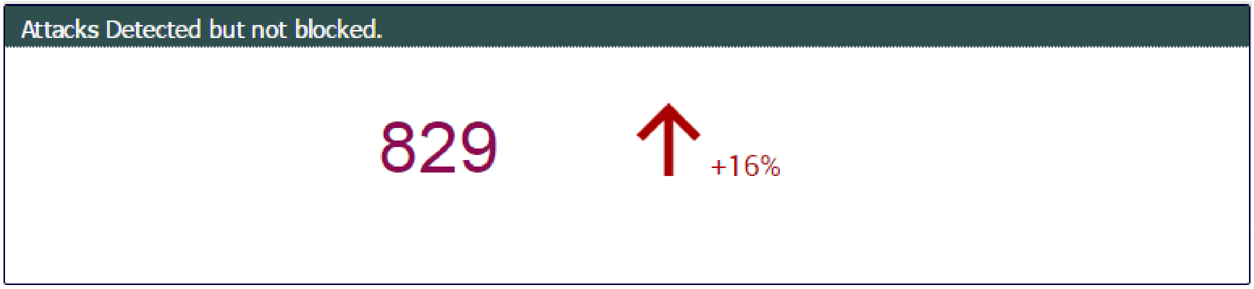
Attacks Detected but not blocked.

Suppose some IPS signatures are configured in Detect mode. Then this number will show how many attacks were detected by Check Point IPS in specified time.

You will also notice an arrow which will show if the attacks were less/more compared to last period.

For example if your setting for Time to Display is default (60 mins) and you ran this app at 3:38PM then upward arrow means that as compared to attacks between 1:38PM - 2:38PM the attacks between

2:38PM - 3:38PM has gone up.

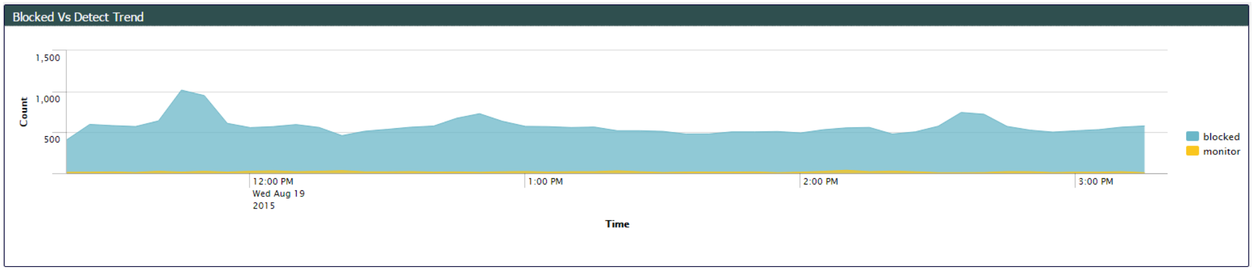


Attacks Detected but not blocked.

829 ↑ +16%

Blocked Vs Detect Trend

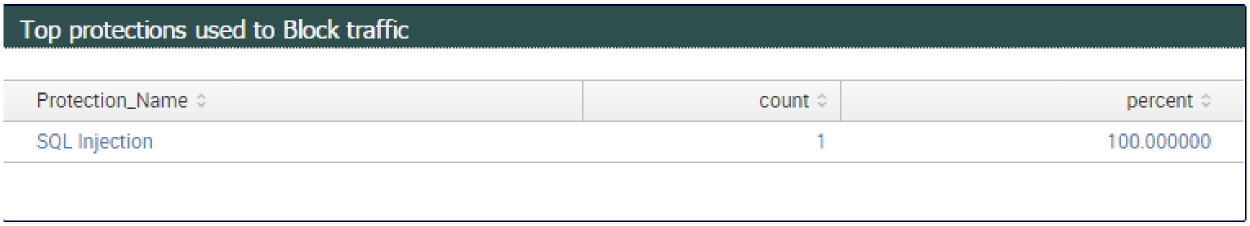
You can observe the trend between IPS Blocked and Detected rate.



Blocked Vs Detect Trend

Top protections used to Block traffic

This window will display the list of top **blocked** protections based on the number of count they were noticed in Check Point IPS logs.

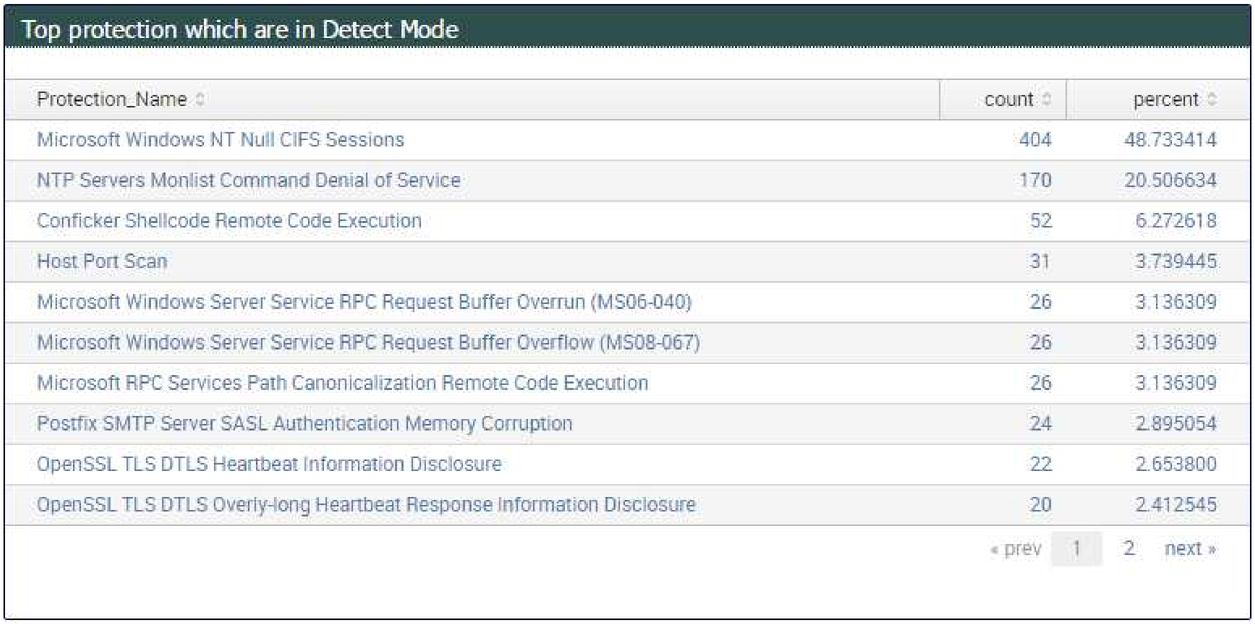


Top protections used to Block traffic

Protection_Name ⇕	count ⇕	percent ⇕
SQL Injection	1	100.000000

Top protection which are in Detect Mode

This window will display the list of top **detected** protections based on the number of count they were noticed in Check Point IPS logs.



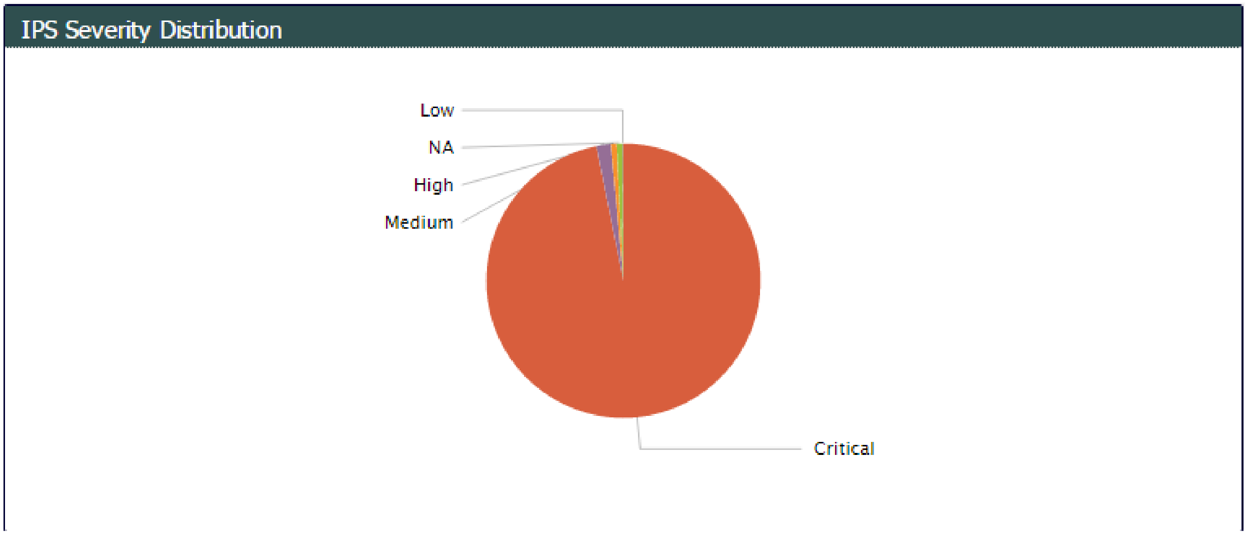
Top protection which are in Detect Mode

Protection_Name	count	percent
Microsoft Windows NT Null CIFS Sessions	404	48.733414
NTP Servers Monlist Command Denial of Service	170	20.506634
Conficker Shellcode Remote Code Execution	52	6.272618
Host Port Scan	31	3.739445
Microsoft Windows Server Service RPC Request Buffer Overrun (MS06-040)	26	3.136309
Microsoft Windows Server Service RPC Request Buffer Overflow (MS08-067)	26	3.136309
Microsoft RPC Services Path Canonicalization Remote Code Execution	26	3.136309
Postfix SMTP Server SASL Authentication Memory Corruption	24	2.895054
OpenSSL TLS DTLS Heartbeat Information Disclosure	22	2.653800
OpenSSL TLS DTLS Overly-long Heartbeat Response Information Disclosure	20	2.412545

IPS Severity Distribution

Each IPS signature is tagged by Check Point based on severity of the attack. This window will show pie chart based on Severity Distribution of IPS attacks.

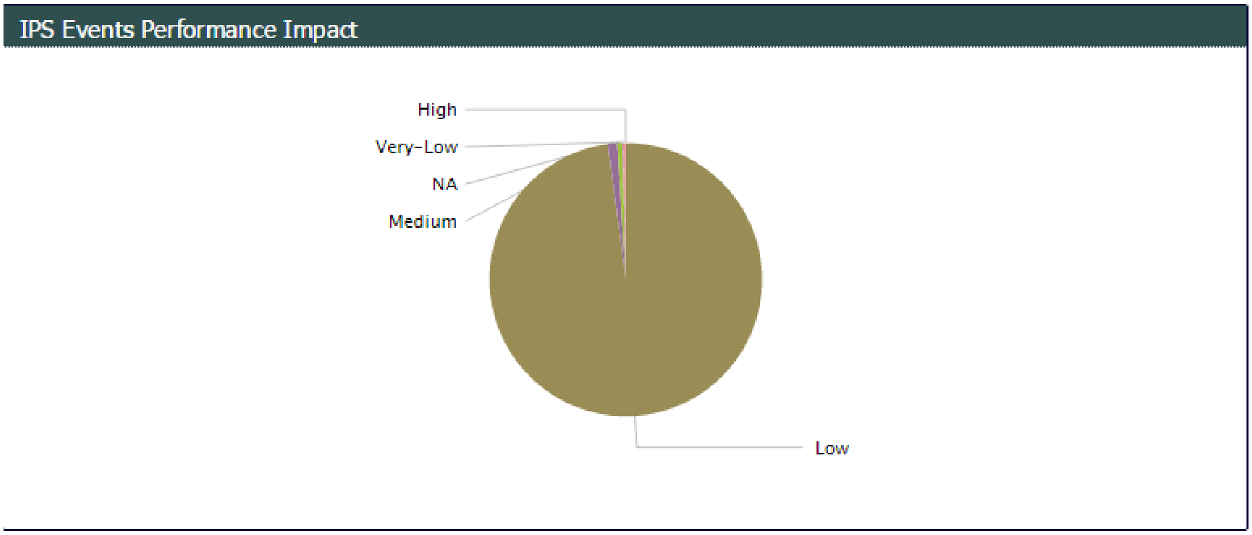
If you notice too many critical attacks (more than 50%) then that should be a matter of concern. You may have to change your IPS policies to make sure your data is not compromised.



IPS Severity Distribution

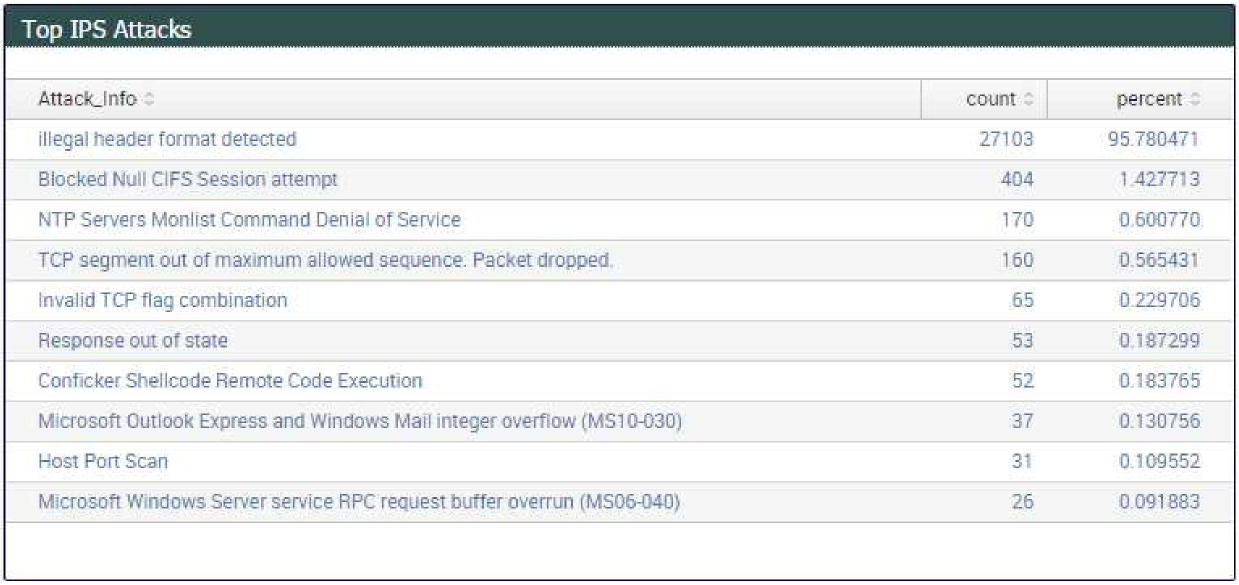
IPS Events Performance Impact

Every IPS signature in Check Point IPS is tagged based on performance impact it will have on Gateway. This window will show a pie chart based on all attacks (detect or blocked).



Top IPS Attacks

Top IPS attacks based on number of times these attacks are catched by Check Point IPS blade.



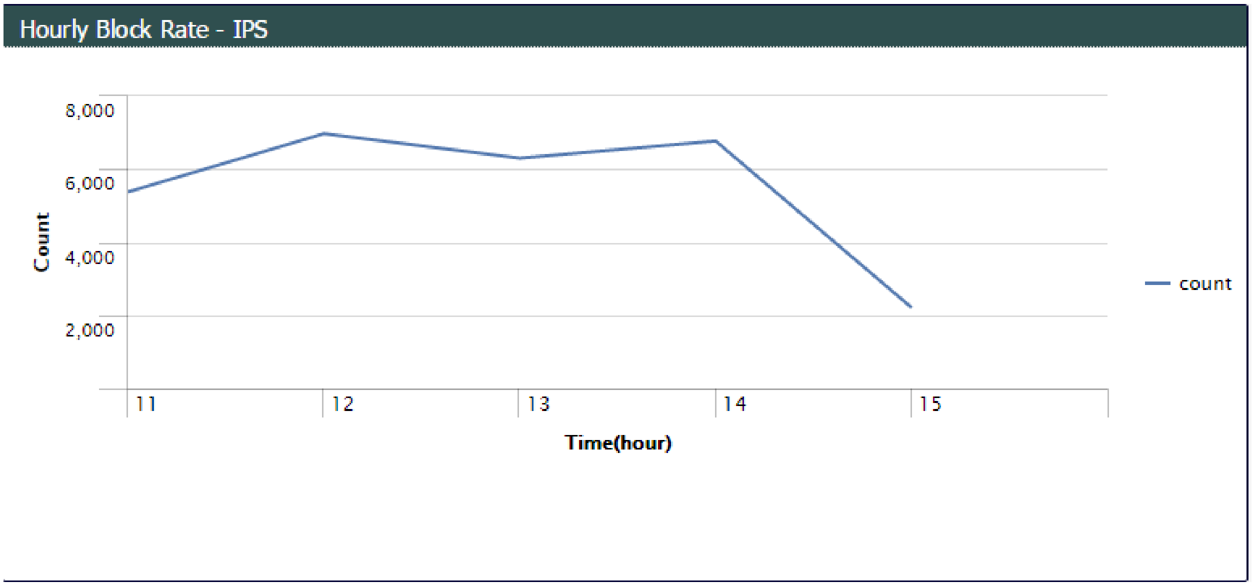
Top IPS Attacks

Attack_Info	count	percent
illegal header format detected	27103	95.780471
Blocked Null CIFS Session attempt	404	1.427713
NTP Servers Monlist Command Denial of Service	170	0.600770
TCP segment out of maximum allowed sequence. Packet dropped.	160	0.565431
Invalid TCP flag combination	65	0.229706
Response out of state	53	0.187299
Conficker Shellcode Remote Code Execution	52	0.183765
Microsoft Outlook Express and Windows Mail integer overflow (MS10-030)	37	0.130756
Host Port Scan	31	0.109552
Microsoft Windows Server service RPC request buffer overrun (MS06-040)	26	0.091883

Hourly Block Rate - IPS

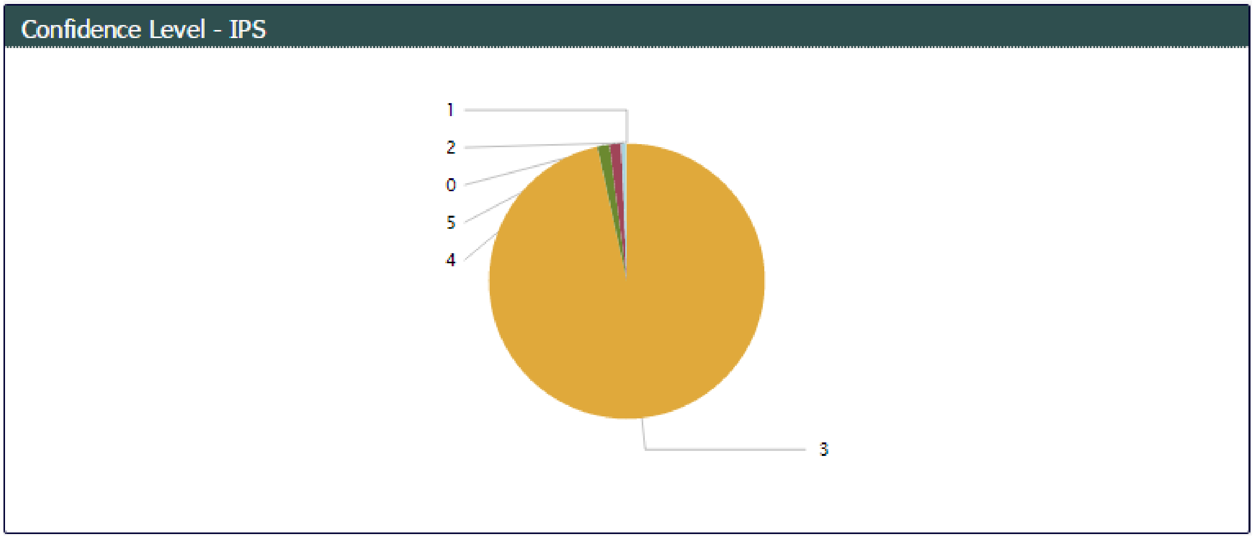
This window will display how many attacks were **blocked** on per hour basis by Check Point IPS.

You may have to choose appropriate Time to Display option to get some useful data. For example you can choose last 4 hrs or last 24 hrs.



Confidence Level - IPS

Check Point IPS signatures are tagged with confidence level. This window will display the pie chart based on confidence level of IPS signatures which were used while Check Point trying to detect or block external threats.

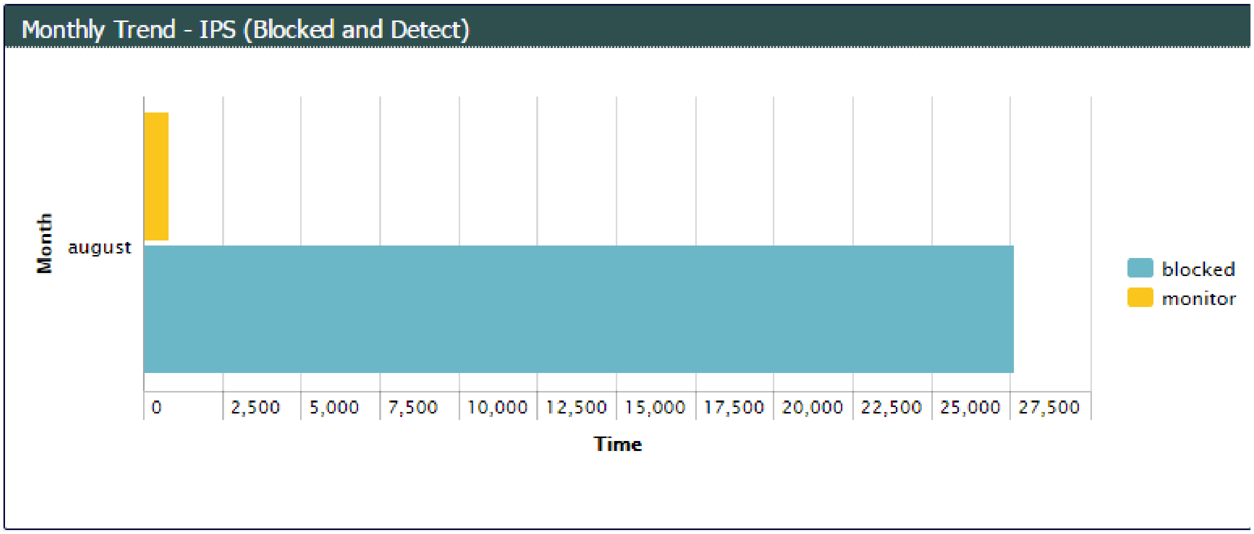


Monthly Trend - IPS (Blocked and Detect)

You will get information about how many attacks were blocked against how many attacks were Detect on month on month basis.

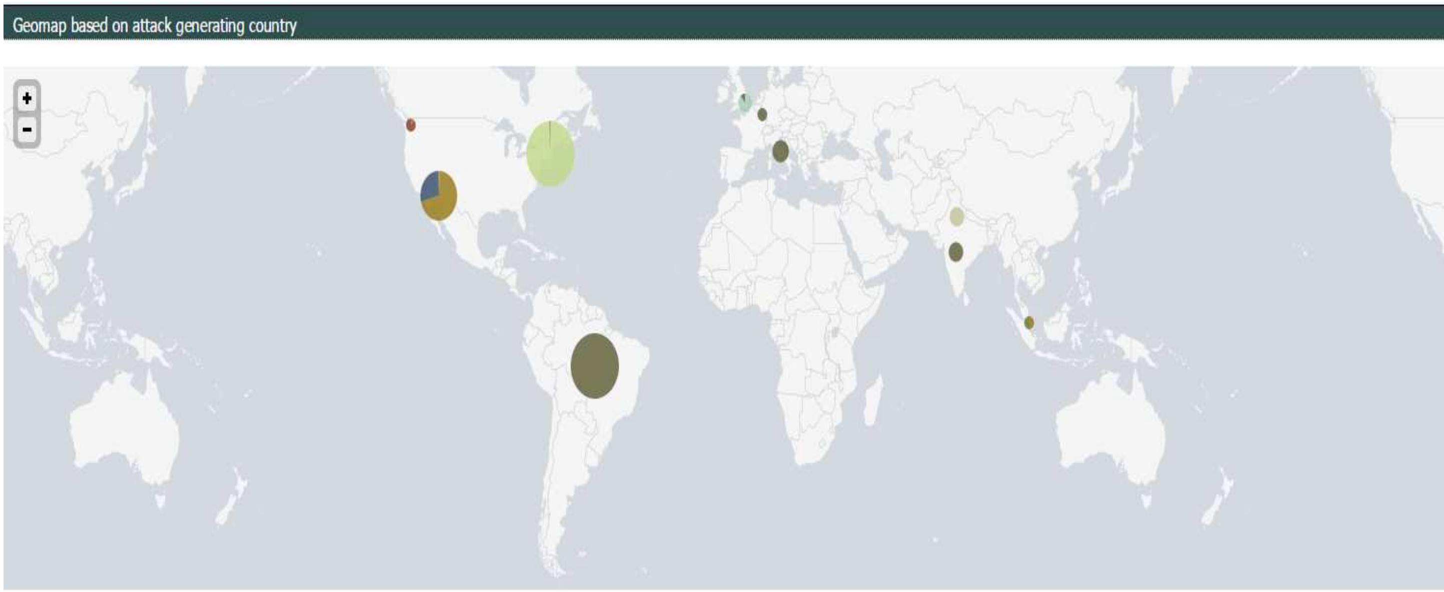
Please note that you will need to change the "Time to Display" at top appropriately so as to include data from more than 1 month.

For example if you choose the time to display as last 30 days and your current data is 15 Aug 2015 then you will data for July 16 - 31 and August 1 - 15.



Geomap based on attack generating country

Will highlight the countries which are attacking your network from internet.

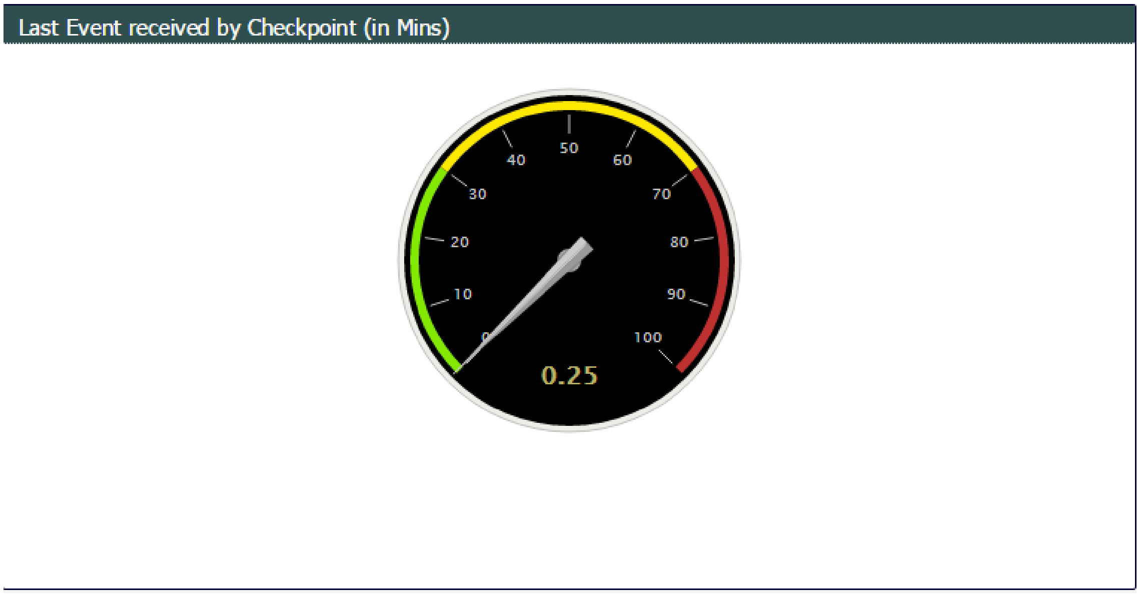

Geomap based on attack generating country

ALERTS

Last Event received by Checkpoint (in Mins)

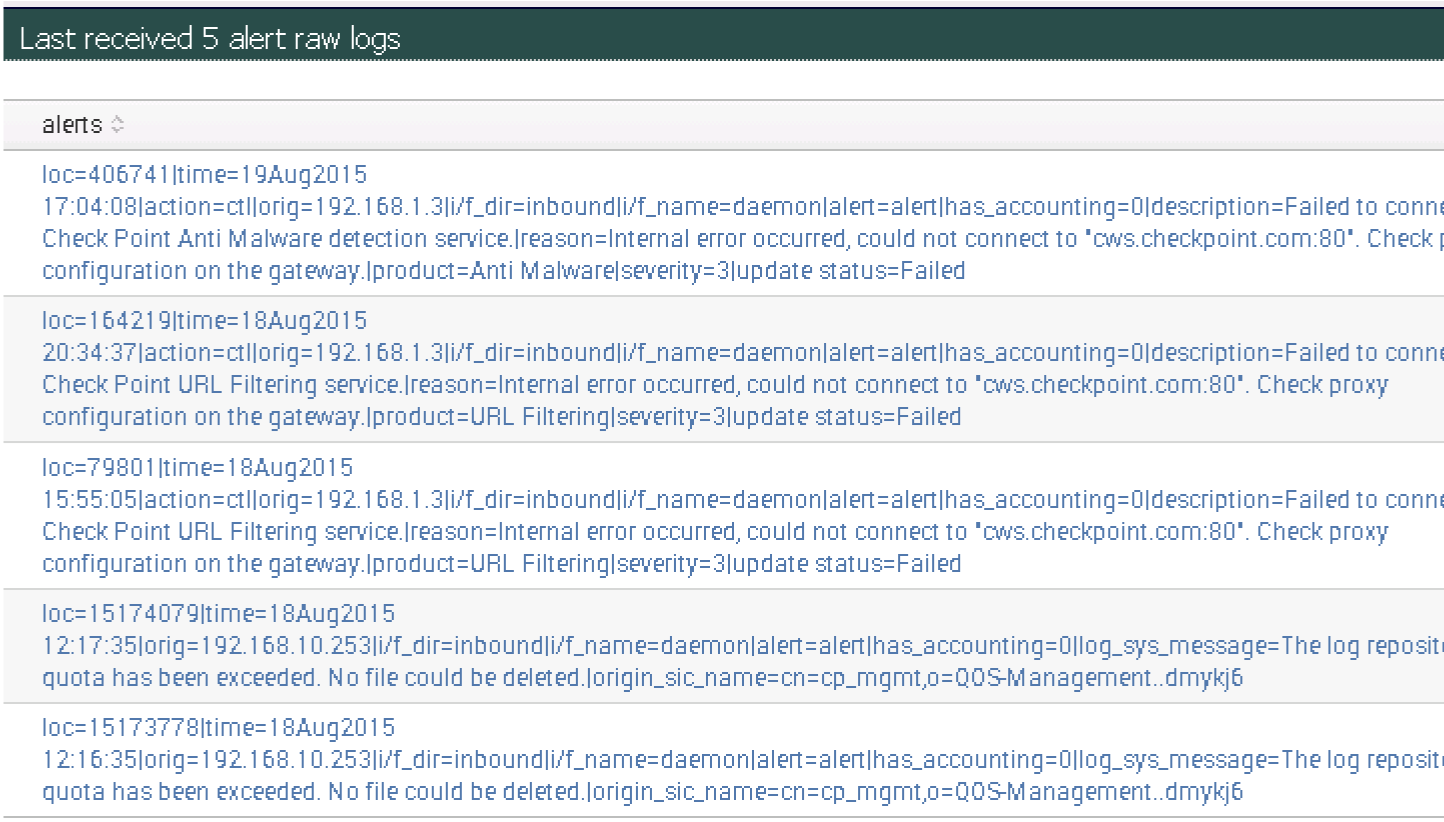
This radial icon will makes sure whether your Splunk Enterprise is receiving the Check Point logs using Check Point LEA client appropriately or not.

Under normal circumstances you will notice the needle well below 1 mins. For some reasons if Check Point stops sending logs to Splunk the needle will move towards red corner indicating the communication problem between Splunk and Check Point Management Server/Log Server.


Last Event received by Checkpoint (in Mins)

Last received 5 alert raw logs

You get latest 5 alerts which are generated by Check Point Management server. These alerts could be related to Disk Space issue, Cluster issue or licensing issue etc.

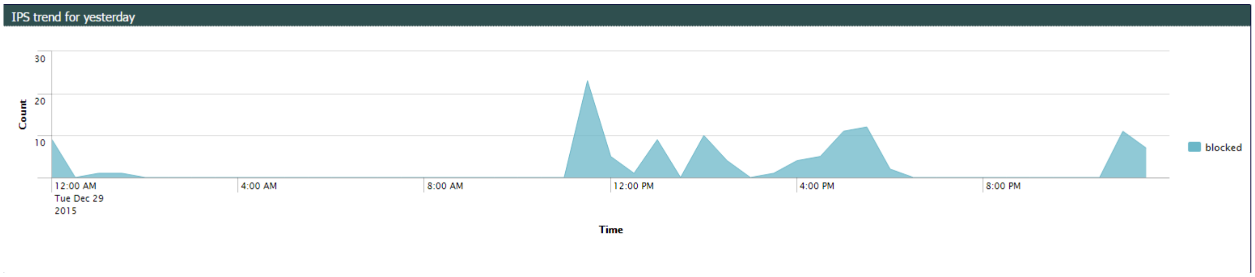


Last received 5 alert raw logs

```
alerts
loc=406741|time=19Aug2015
17:04:08|action=ctl|orig=192.168.1.3|i/f_dir=inbound|i/f_name=daemon|alert=alert|has_accounting=0|description=Failed to conne
Check Point Anti Malware detection service.|reason=Internal error occurred, could not connect to 'cws.checkpoint.com:80'. Check p
configuration on the gateway.|product=Anti Malware|severity=3|update status=Failed
loc=164219|time=18Aug2015
20:34:37|action=ctl|orig=192.168.1.3|i/f_dir=inbound|i/f_name=daemon|alert=alert|has_accounting=0|description=Failed to conne
Check Point URL Filtering service.|reason=Internal error occurred, could not connect to 'cws.checkpoint.com:80'. Check proxy
configuration on the gateway.|product=URL Filtering|severity=3|update status=Failed
loc=79801|time=18Aug2015
15:55:05|action=ctl|orig=192.168.1.3|i/f_dir=inbound|i/f_name=daemon|alert=alert|has_accounting=0|description=Failed to conne
Check Point URL Filtering service.|reason=Internal error occurred, could not connect to 'cws.checkpoint.com:80'. Check proxy
configuration on the gateway.|product=URL Filtering|severity=3|update status=Failed
loc=15174079|time=18Aug2015
12:17:35|orig=192.168.10.253|i/f_dir=inbound|i/f_name=daemon|alert=alert|has_accounting=0|log_sys_message=The log reposit
quota has been exceeded. No file could be deleted.|origin_sic_name=cn=cp_mgmt,o=QOS-Management..dmykj6
loc=15173778|time=18Aug2015
12:16:35|orig=192.168.10.253|i/f_dir=inbound|i/f_name=daemon|alert=alert|has_accounting=0|log_sys_message=The log reposit
quota has been exceeded. No file could be deleted.|origin_sic_name=cn=cp_mgmt,o=QOS-Management..dmykj6
```

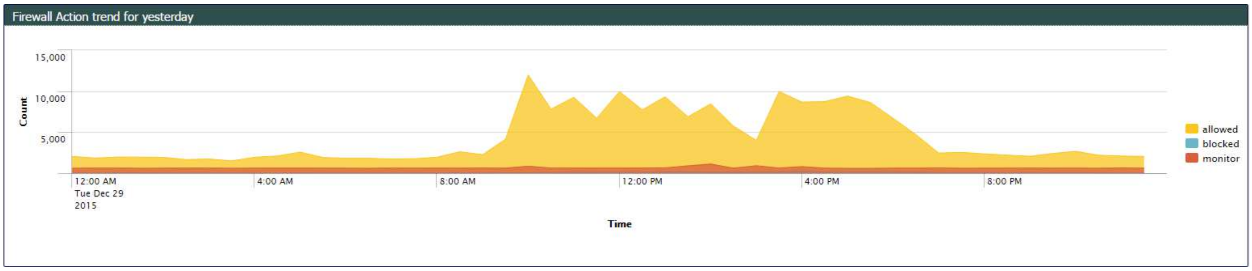
IPS trend for yesterday

Sometimes you need to see the trend of IPS logs on a typical 24 hrs. This window will give you IPS log trends for yesterday's 24 hrs. Suppose you are running the app on 23rd Dec 2015 around 10AM. Then this window will provide you trend for IPS logs between 22nd Dec 2015 0000 hrs till 22nd Dec 2015 2359 hrs.



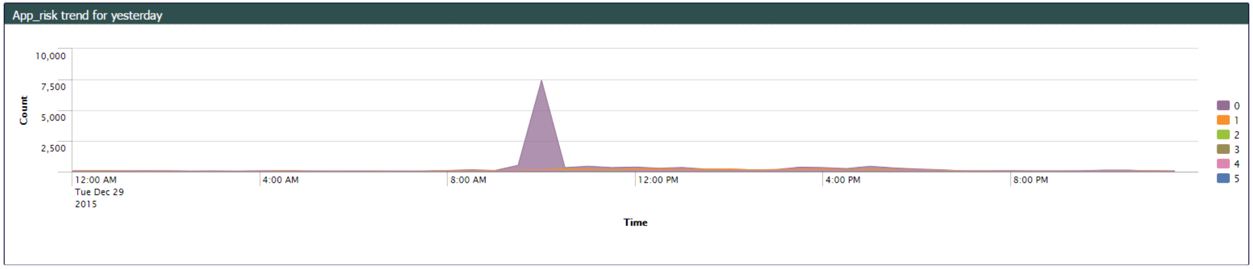
Firewall Action trend for yesterday

Sometimes you need to see the trend of Firewall logs on a typical 24 hrs. This window will give you Firewall log trends for yesterday's 24 hrs. Suppose you are running the app on 23rd Dec 2015 around 10AM. Then this window will provide you trend for IPS logs between 22nd Dec 2015 0000 hrs till 22nd Dec 2015 2359 hrs.



App_risk trend for yesterday

Sometimes you need to see the trend of App and URL logs based on their risk score on a typical 24 hrs. This window will give you App and URL log trends for yesterday's 24 hrs . Suppose you are running the app on 23rd Dec 2015 around 10AM. Then this window will provide you trend for IPS logs between 22nd Dec 2015 0000 hrs till 22nd Dec 2015 2359 hrs.



Last received 5 critical cluster info

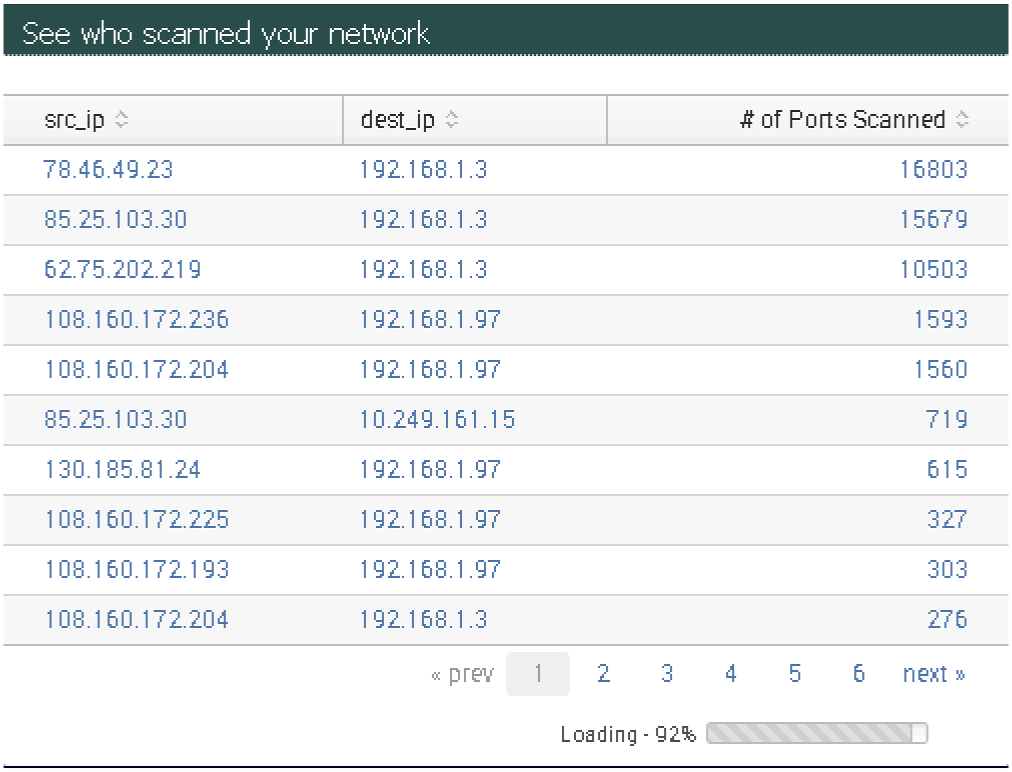
In this window you will notice any logs generated by Check Point clusterXL feature. Most of the times we have noticed that production clusterXL failover for some reason or the other. This window will provide details about such issues with clusterXL.

See who scanned your network

This shows the list of IP address who have scanned your network from Internet.

Ideally you should block these IP addresses in Firewall Rule base or IPS Geo policy of Check Point.

Any ip which is not from the range 10.0.0.0/8, 172.16.0.0/12 & 192.168.0.0/16 [RFC 1918] is considered external IP Address.

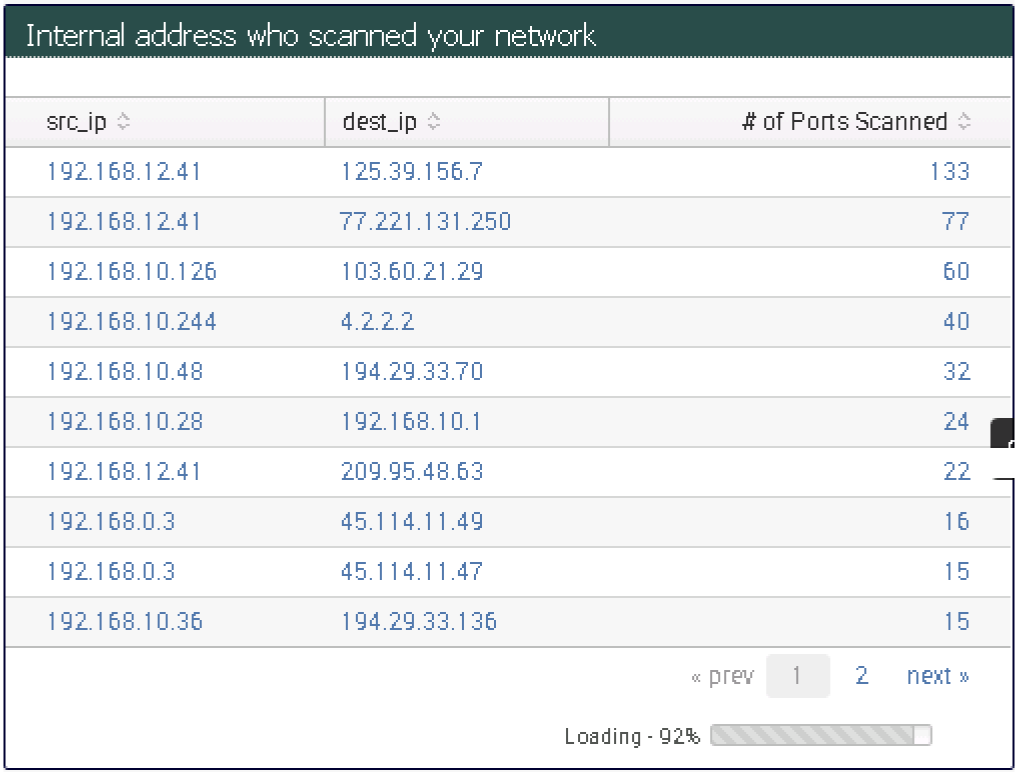


See who scanned your network

src_ip	dest_ip	# of Ports Scanned
78.46.49.23	192.168.1.3	16803
85.25.103.30	192.168.1.3	15679
62.75.202.219	192.168.1.3	10503
108.160.172.236	192.168.1.97	1593
108.160.172.204	192.168.1.97	1560
85.25.103.30	10.249.161.15	719
130.185.81.24	192.168.1.97	615
108.160.172.225	192.168.1.97	327
108.160.172.193	192.168.1.97	303
108.160.172.204	192.168.1.3	276

Internal address who scanned your network

This is list the local IP addresses which were found performing port scanning. These are local IP addresses in the range 10.0.0.0/8, 172.16.0.0/12 & 192.168.0.0/16 [RFC 1918].



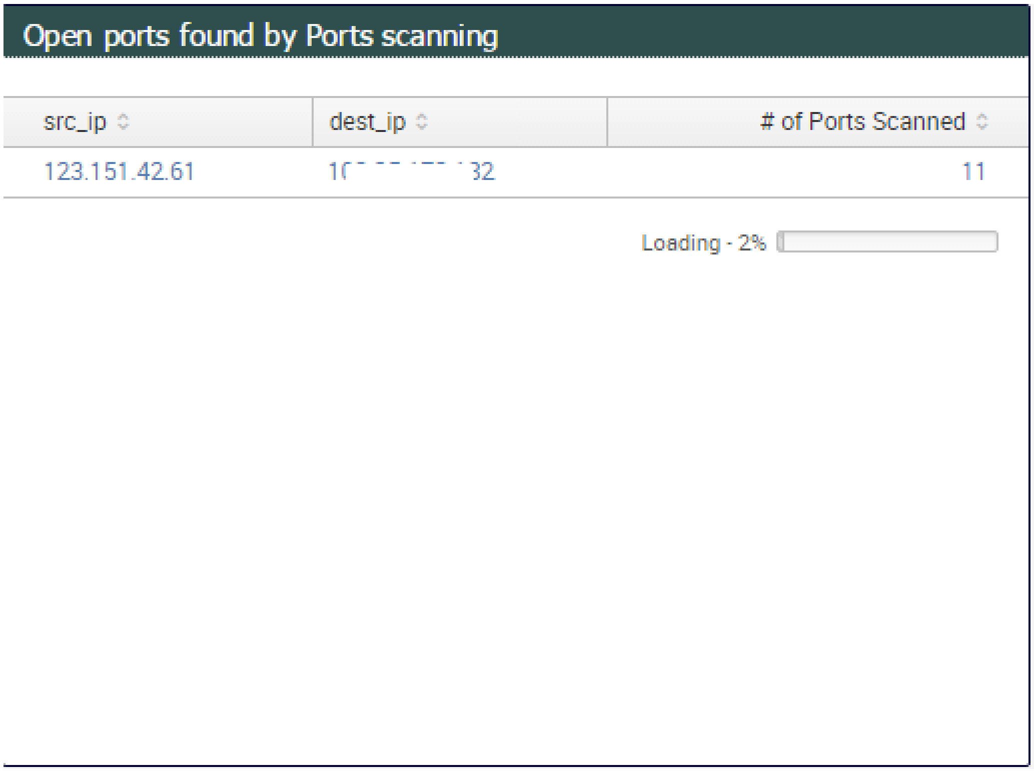
Internal address who scanned your network

src_ip	dest_ip	# of Ports Scanned
192.168.12.41	125.39.156.7	133
192.168.12.41	77.221.131.250	77
192.168.10.126	103.60.21.29	60
192.168.10.244	4.2.2.2	40
192.168.10.48	194.29.33.70	32
192.168.10.28	192.168.10.1	24
192.168.12.41	209.95.48.63	22
192.168.0.3	45.114.11.49	16
192.168.0.3	45.114.11.47	15
192.168.10.36	194.29.33.136	15

Open ports found by Ports scanning

If you see some IP addresses here that means someone has scanned your network and found open ports. These ports are allowed in Firewall Rule base.

Ideally you should block these IP addresses in Firewall Rule base or IPS Geo policy of Check Point.



Open ports found by Ports scanning

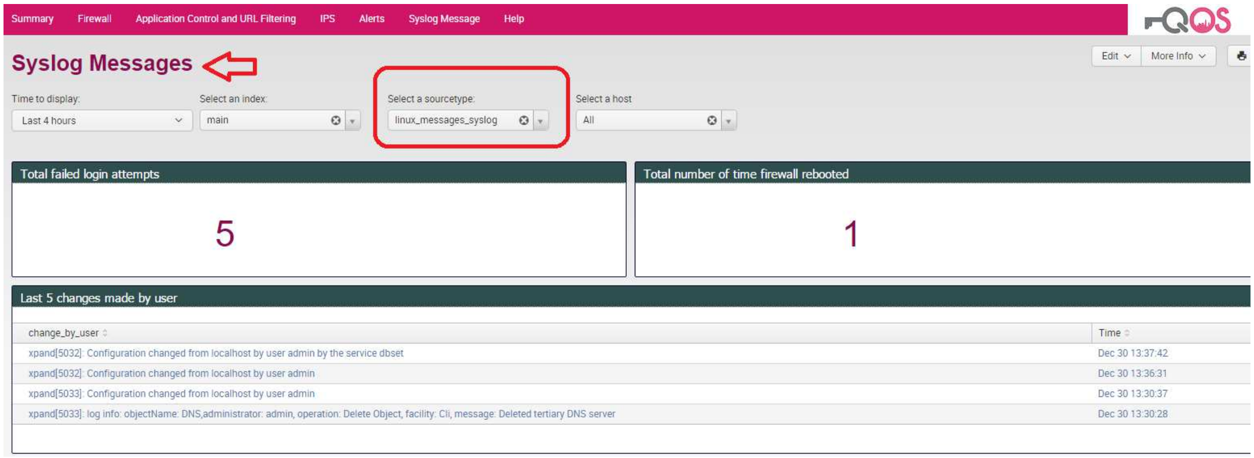
src_ip	dest_ip	# of Ports Scanned
123.151.42.61	[redacted]	11

SYSLOG MESSAGE

Unlike other Tabs such as Summary, Firewall & IPS this tab uses a different sourcetype to display analytics. Purpose of this feature is to capture Check Point Gaia Syslog messages and provide some very useful information at single place. In order to use this feature please follow the steps mentioned below.

Steps to configure Check Point syslog capture.

1. Open ssh to Check Point Gaia Management Server or Gateway.
2. In normal user mode run following command.
   - CPFW> add syslog log-remote-address <your-splunk-ip-address> level info
   - CPFW> save config
3. Login to Splunk. Click Settings-> Data Input -> Local inputs (UDP) -> Add new
4. Provide necessary details and save.
5. Now whatever sourcetype name you are going to create in step 13, you need to mention the same in /opt/splunk/etc/apps/CheckPointAnalyticsAppbyQOS/default/props.conf
6. By default we have given a temporary sourcetype = qos_syslog.
7. Change the temporary sourcetype once you have successfully installed this app. No need to restart Splunk after making changes to props.conf as suggested in step 5.
8. Now you can choose appropriate sourcetype for syslog messages to get required result. In below screen shot I have used sourcetype as linux_messages_syslog.



Syslog Messages

Time to display: Last 4 hours

Select an index: main

Select a sourcetype: linux_messages_syslog

Select a host: All

Total failed login attempts

5

Total number of time firewall rebooted

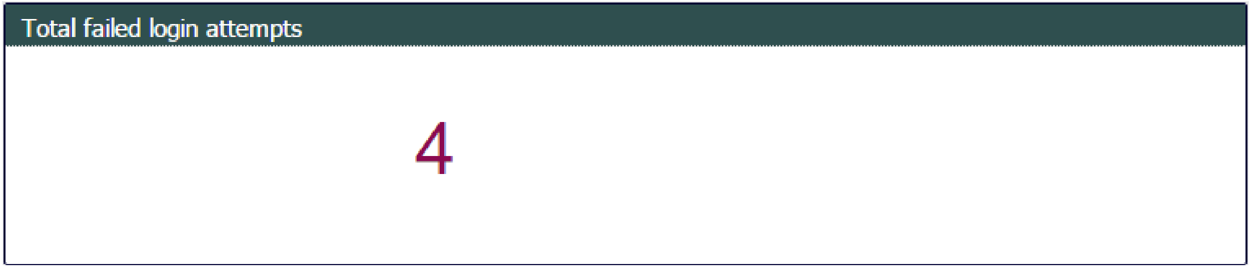
1

Last 5 changes made by user

change_by_user	Time
xpand[5032]: Configuration changed from localhost by user admin by the service dbset	Dec 30 13:37:42
xpand[5032]: Configuration changed from localhost by user admin	Dec 30 13:36:31
xpand[5033]: Configuration changed from localhost by user admin	Dec 30 13:30:37
xpand[5033]: log info: objectName: DNS,administrator: admin, operation: Delete Object, facility: Cli, message: Deleted tertiary DNS server	Dec 30 13:30:28

Total failed login attempts

Now find out how many failed login attempts were there on your Check Point devices. A very high number here telling you that someone trying to gain unauthorized access.

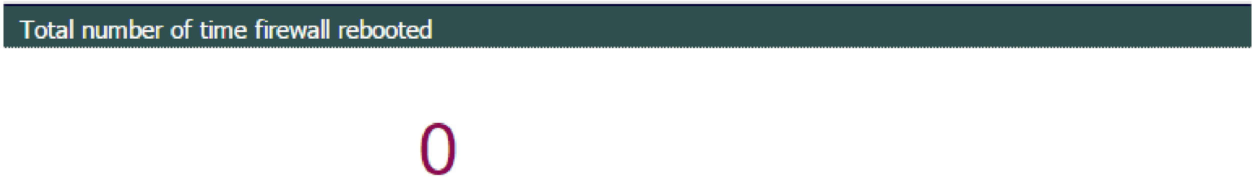


Total failed login attempts

4

Total number of time firewall rebooted

Sometimes your firewall reboots automatically. This could happen due to manual intervention but many times it could be due to power or other issues.

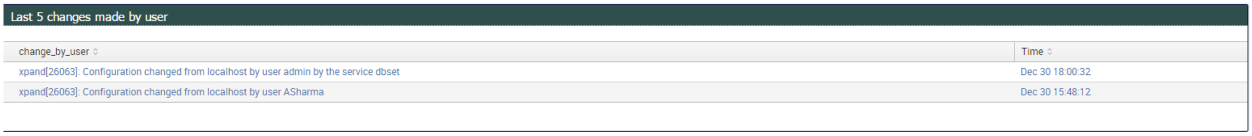


Total number of time firewall rebooted

0

Last 5 changes made by user

Find out who had made changes on Check Point Management server or on Gateways running Gaia OS.

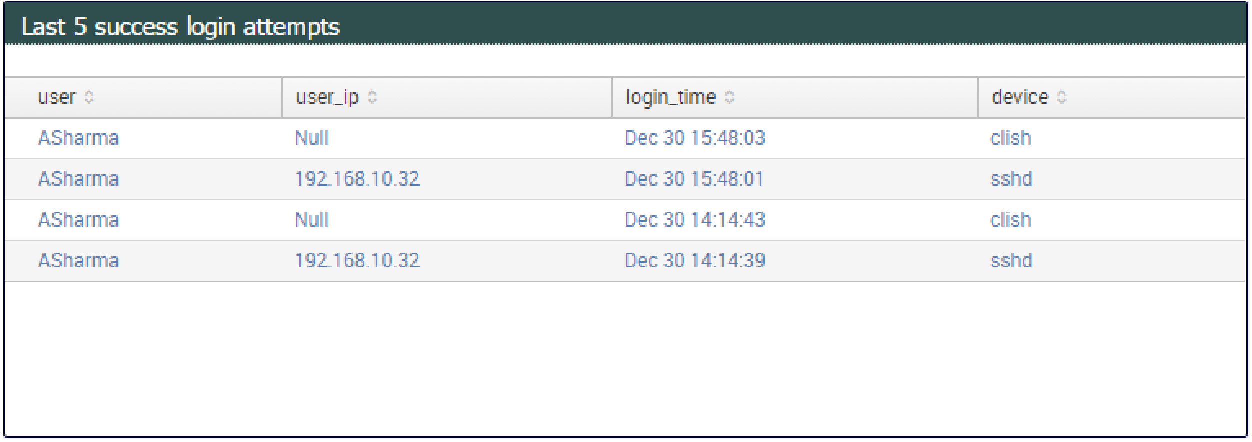


Last 5 changes made by user

change_by_user	Time
xpand[26063]: Configuration changed from localhost by user admin by the service dbset	Dec 30 18:00:32
xpand[26063]: Configuration changed from localhost by user ASharma	Dec 30 15:48:12

Last 5 success login attempts

It is also a good practice to capture successful login attempts as well. If you see successful login from unknow IP address at suspicious time you know that something is definitely wrong.

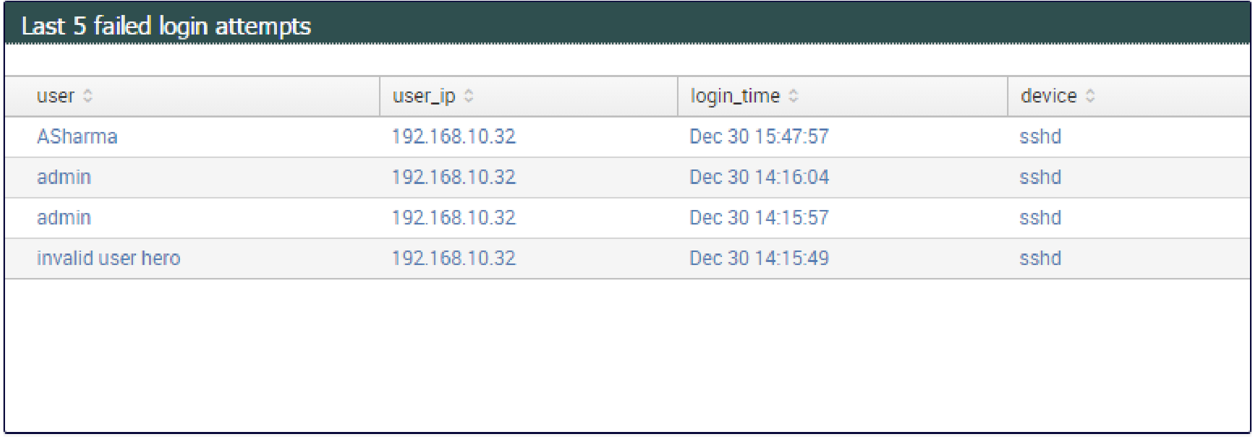


Last 5 success login attempts

user	user_ip	login_time	device
ASharma	Null	Dec 30 15:48:03	clish
ASharma	192.168.10.32	Dec 30 15:48:01	sshd
ASharma	Null	Dec 30 14:14:43	clish
ASharma	192.168.10.32	Dec 30 14:14:39	sshd

Last 5 failed login attempts

List of users and IP addresses from where failed login attempts were captured.

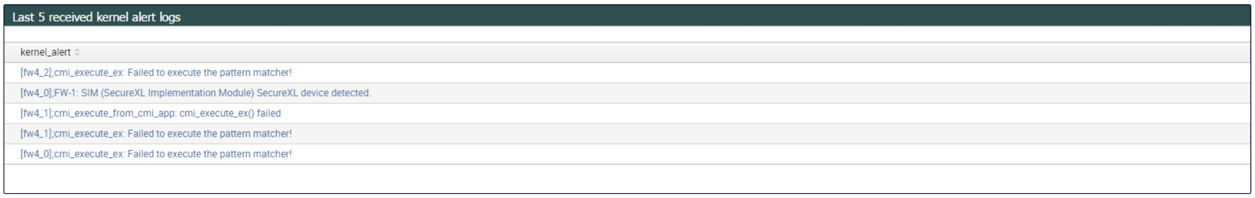


Last 5 failed login attempts

user	user_ip	login_time	device
ASharma	192.168.10.32	Dec 30 15:47:57	sshd
admin	192.168.10.32	Dec 30 14:16:04	sshd
admin	192.168.10.32	Dec 30 14:15:57	sshd
invalid user hero	192.168.10.32	Dec 30 14:15:49	sshd

Last 5 received kernel alert logs

Under normal circumstanced you should not see any kernel level messages in /var/log/messages file on your Check Point devices. If there are kernel level errors please work with Check Point to fix the issue.

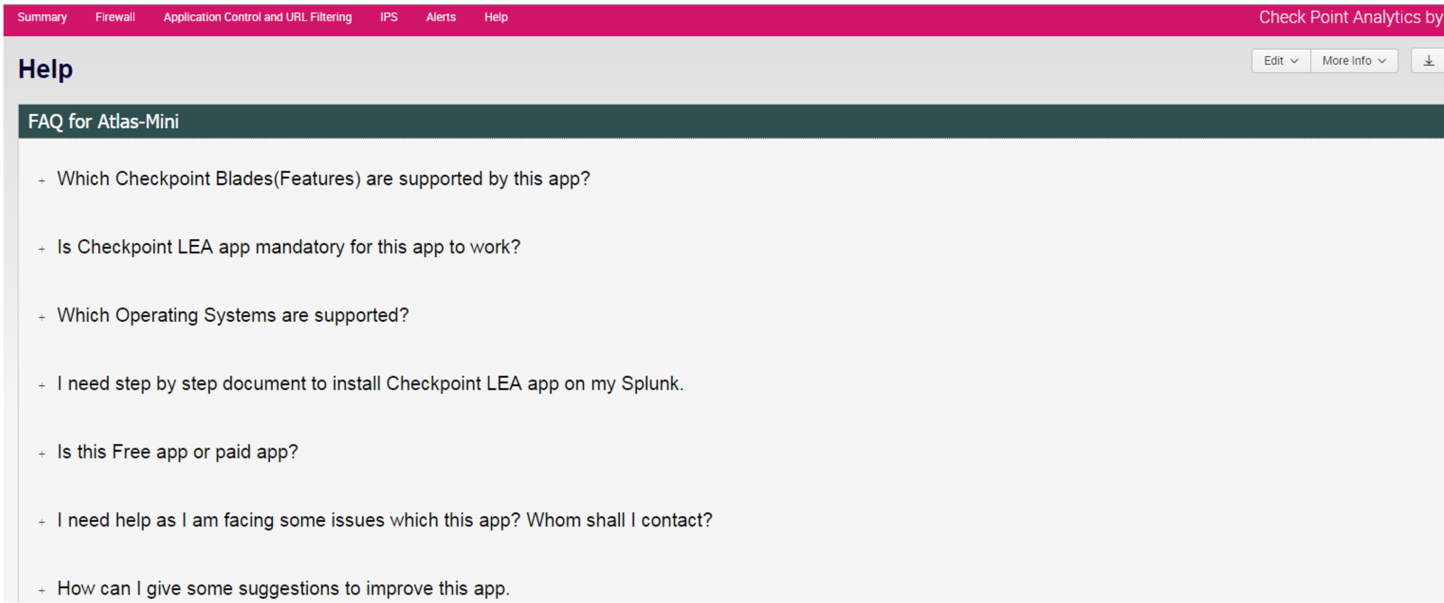


Last 5 received kernel alert logs

kernel_alert
[fw4_2];cmi_execute_ex: Failed to execute the pattern matcher!
[fw4_0];FW-1: SIM (SecureXL Implementation Module) SecureXL device detected.
[fw4_1];cmi_execute_from_cmi_app: cmi_execute_ex() failed
[fw4_1];cmi_execute_ex: Failed to execute the pattern matcher!
[fw4_0];cmi_execute_ex: Failed to execute the pattern matcher!

HELP

This page displays FAQs.



Help

FAQ for Atlas-Mini

- Which Checkpoint Blades(Features) are supported by this app?
- Is Checkpoint LEA app mandatory for this app to work?
- Which Operating Systems are supported?
- I need step by step document to install Checkpoint LEA app on my Splunk.
- Is this Free app or paid app?
- I need help as I am facing some issues which this app? Whom shall I contact?
- How can I give some suggestions to improve this app.