Module 12 System Monitoring

Module 1: System Monitoring

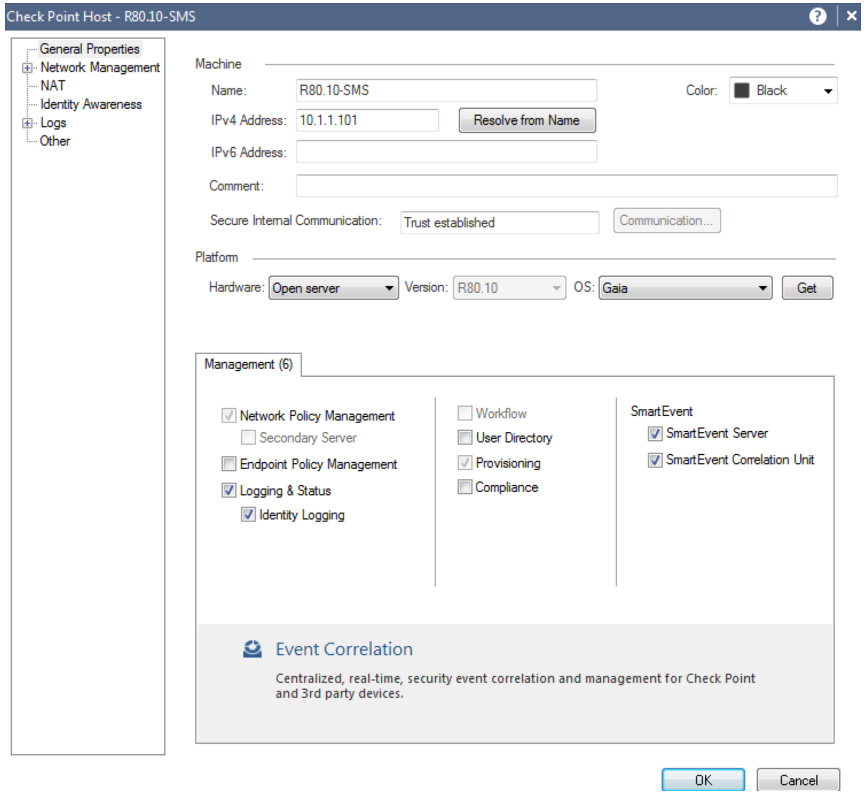
Instructor: Kim Winfield

Objectives

- Use Smart Event and event correlation
- Apply Smartview Monitor and real time monitoring
- Use CPView to monitor the Security Gateway real time performance and historical performance

SmartEvent

- Event Analysis
- Log Entries are used to create events
- Creating Custom Events



Check Point Host - R80.10-SMS

Machine

Name: R80.10-SMS

Color: Black

IPv4 Address: 10.1.1.101

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Platform

Hardware: Open server Version: R80.10 OS: Gaia

Management (6)

☑ Network Policy Management
☐ Secondary Server
☐ Endpoint Policy Management
☑ Logging & Status
☑ Identity Logging

☐ Workflow
☐ User Directory
☑ Provisioning
☐ Compliance

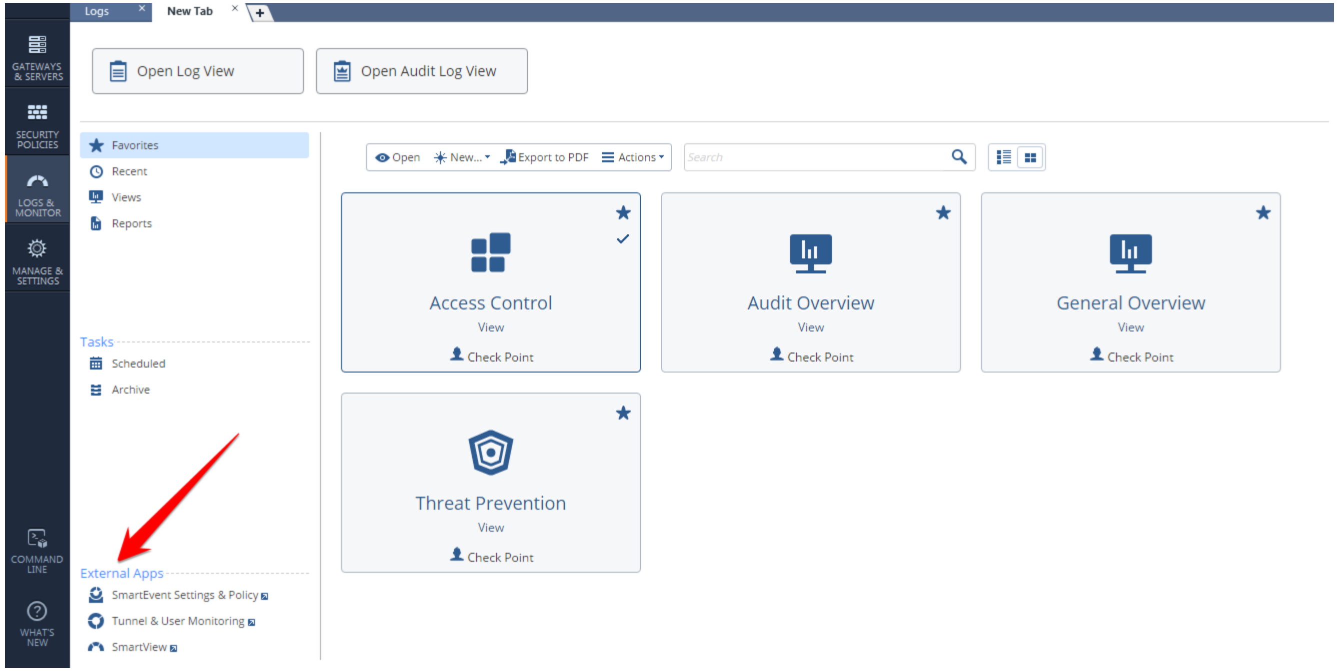
SmartEvent
☑ SmartEvent Server
☑ SmartEvent Correlation Unit

Event Correlation

Centralized, real-time, security event correlation and management for Check Point and 3rd party devices.

SmartEvent

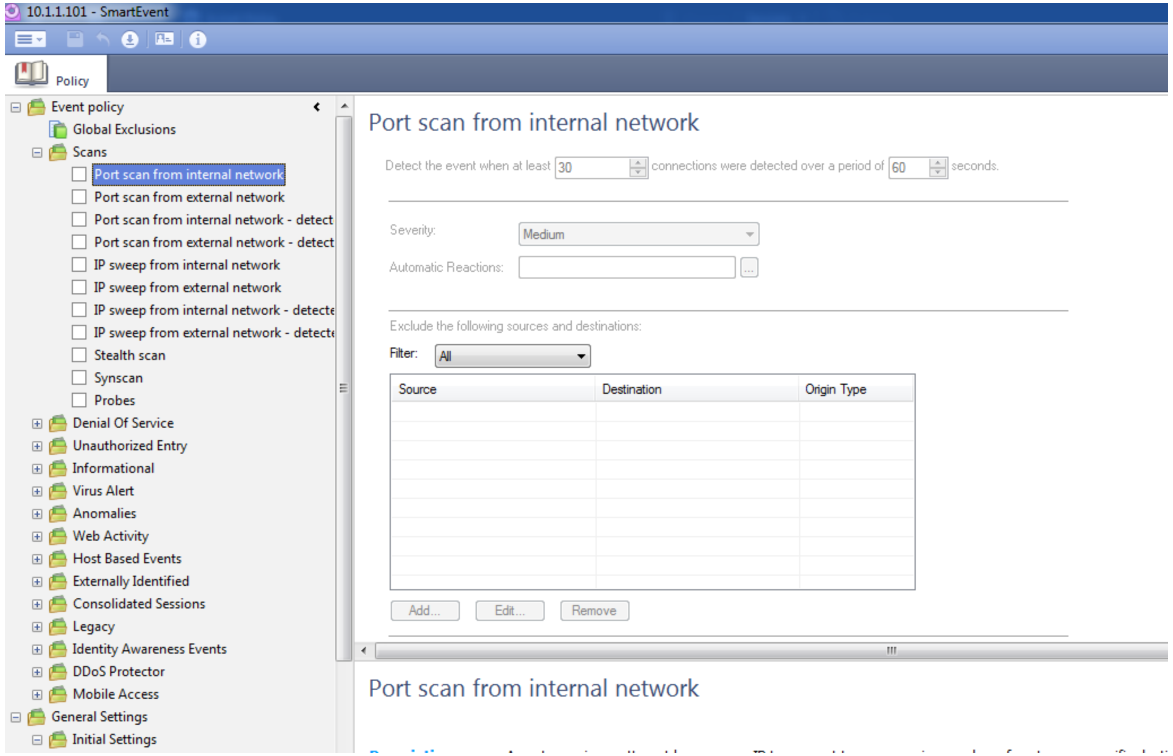
- Log Views and Reports
- Scheduled Tasks
- Archive
- External Apps
  - Smart Event Settings
  - Tunnel &User Monitoring
  - Smarview



SmartEvent Policy

- Event Policy
  - Global Exclusions
  - Network Based Events
  - Malware and Anit-Virus Events
  - Identity Awareness Events
  - Mobile Access Events

- General Settings
  - Initial Settings
  - Objects


10.1.1.101 - SmartEvent
Policy
Event policy
Global Exclusions
Scans
□ Port scan from internal network
□ Port scan from external network
□ Port scan from internal network - detect
□ Port scan from external network - detect
□ IP sweep from internal network
□ IP sweep from external network
□ IP sweep from internal network - detecte
□ IP sweep from external network - detecte
□ Stealth scan
□ Synscan
□ Probes
Denial Of Service
Unauthorized Entry
Informational
Virus Alert
Anomalies
Web Activity
Host Based Events
Externally Identified
Consolidated Sessions
Legacy
Identity Awareness Events
DDoS Protector
Mobile Access
General Settings
Initial Settings
Add...
Edit...
Remove

Port scan from internal network

Detect the event when at least 30 connections were detected over a period of 60 seconds.

Severity: Medium

Automatic Reactions:

Exclude the following sources and destinations:

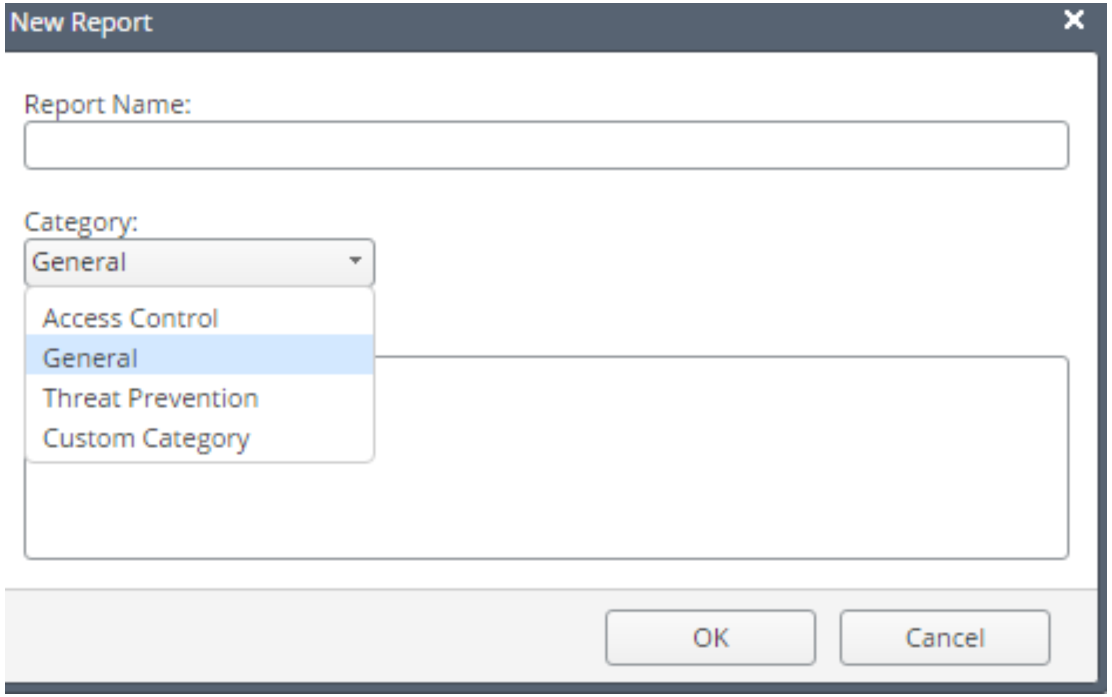
Filter: All

Source	Destination	Origin Type

Port scan from internal network

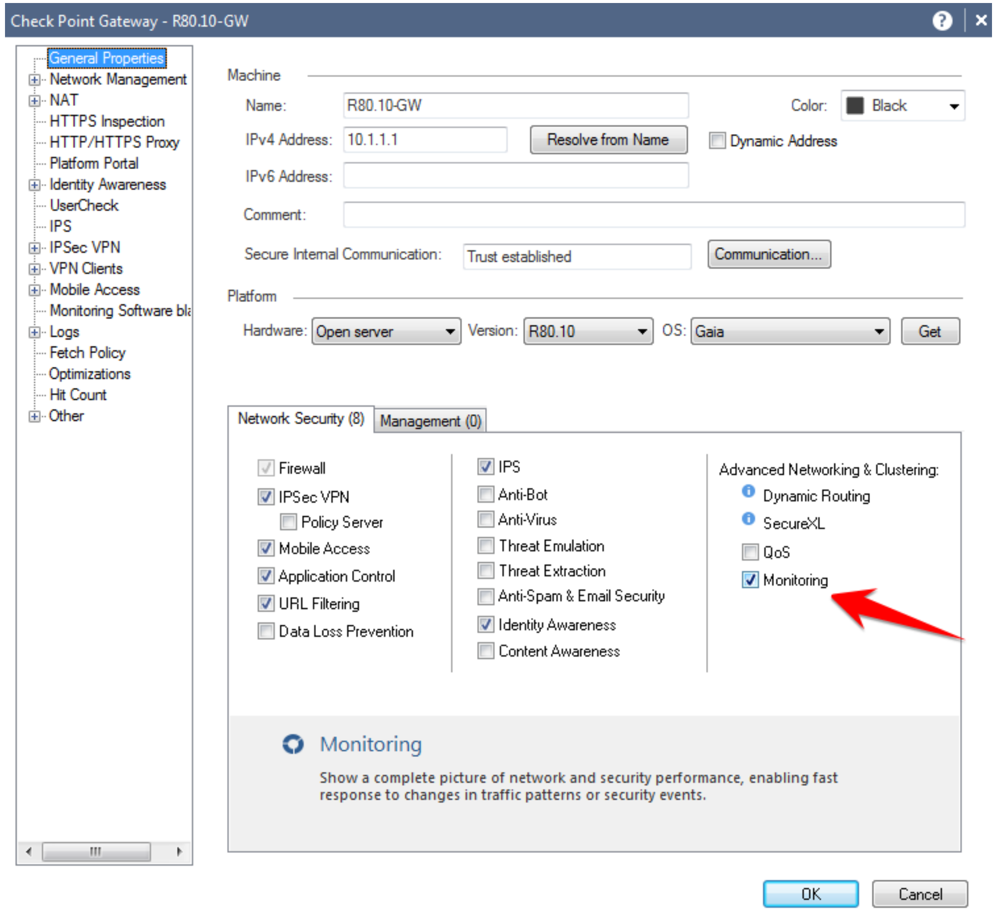
SmartEvent Reports

- Pre-defined Reports
- User Defined View
- User Defined Report



SmartView Monitor

- Monitoring System Health
- Monitoring Traffic
- Enabled on Security Gateway



Machine

Name: R80.10-GW

Color: Black

IPv4 Address: 10.1.1.1

□ Dynamic Address

IPv6 Address:

Comment:

Secure Internal Communication: Trust established

Platform

Hardware: Open server Version: R80.10 OS: Gaia

Network Security (8) | Management (0)

☑ Firewall
☑ IPSec VPN
□ Policy Server
☑ Mobile Access
☑ Application Control
☑ URL Filtering
□ Data Loss Prevention

☑ IPS
□ Anti-Bot
□ Anti-Virus
□ Threat Emulation
□ Threat Extraction
□ Anti-Spam & Email Security
☑ Identity Awareness
□ Content Awareness

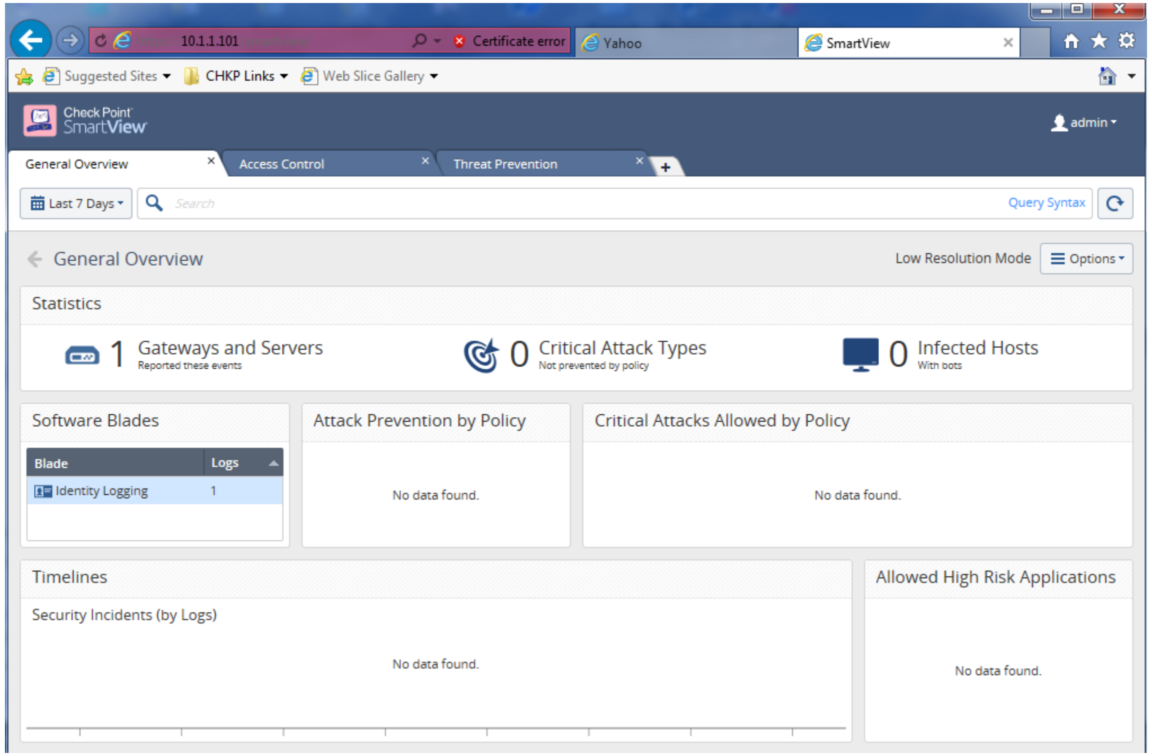
Advanced Networking & Clustering:
Dynamic Routing
SecureXL
□ QoS
☑ Monitoring

Monitoring

Show a complete picture of network and security performance, enabling fast response to changes in traffic patterns or security events.

SmartView Monitor

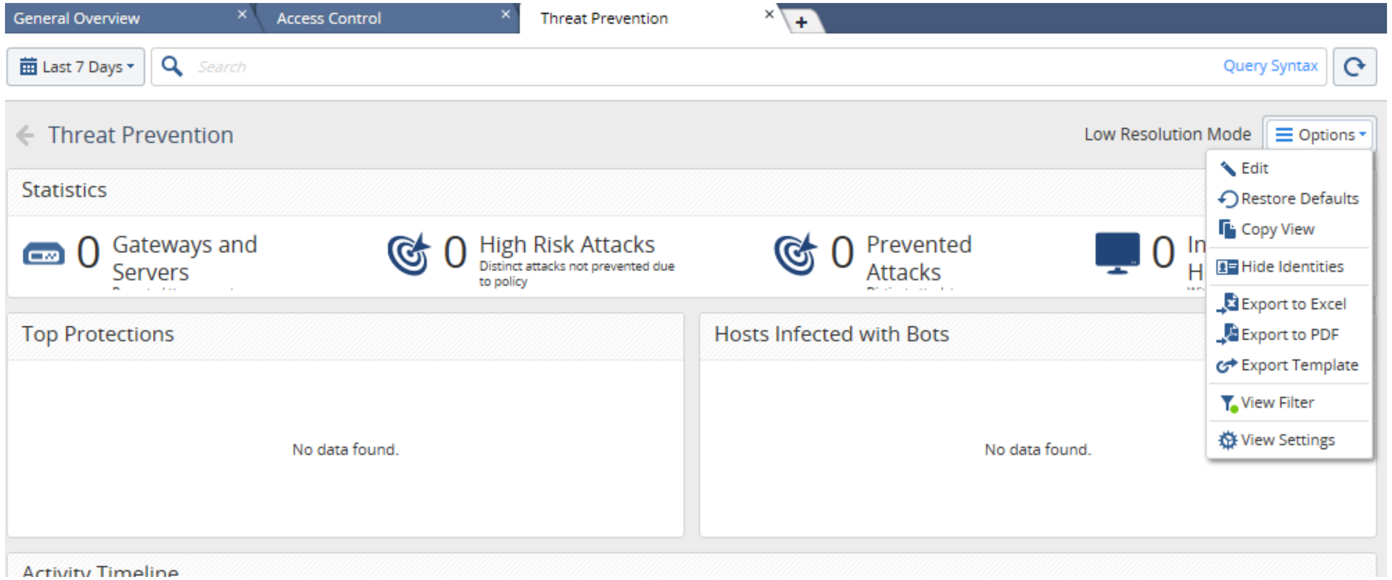
- Web Based Application
- Enable Monitoring on the Gateways
- General Overview
  - Statistics
  - Software Blades
- Access Control
  - Allowed Traffic
  - Blocked Traffic
- Threat Prevention
  - Statistics
  - Top Protections
  - Hosts Infected with Bots



Blade	Logs
Identity Logging	1

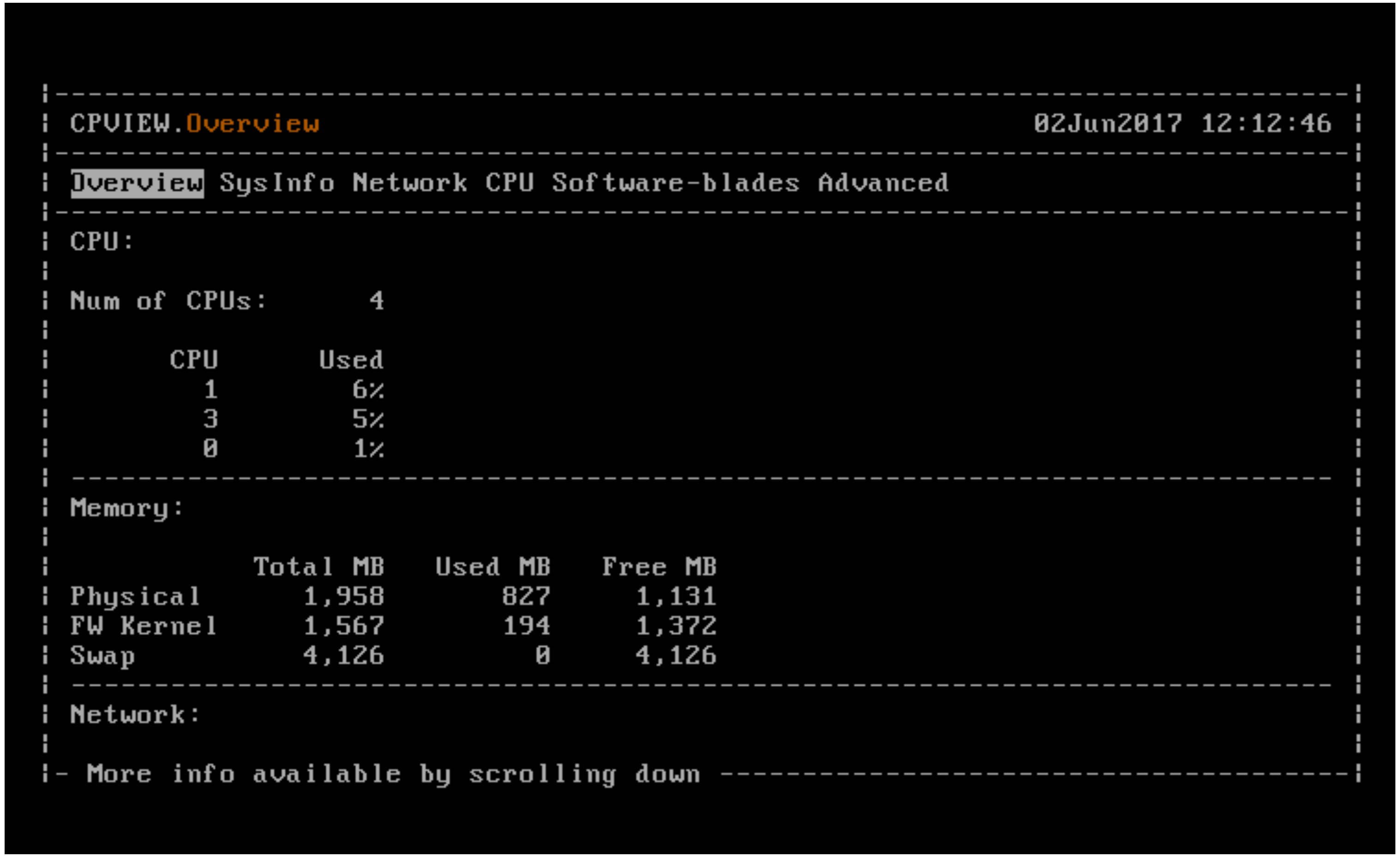
SmartView Monitor

- Options
- Hide Identities of Users
- Export
    - Excel
    - PDF
    - Export Template
- View Settings



CPView

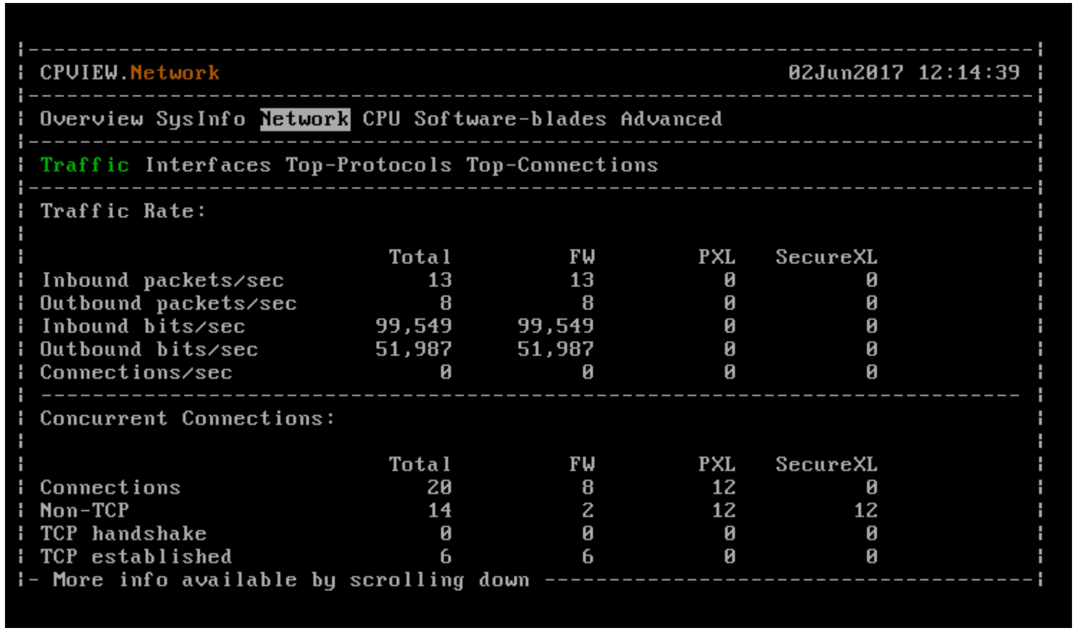
- Shell Menu
- Overview
- System Information
- Network
- CPU
- Software Blades
- Advanced



```
|---------------------------------------------------------------------------------|
| CPVIEW.Overview                                           02Jun2017 12:12:46 |
|---------------------------------------------------------------------------------|
| Overview SysInfo Network CPU Software-blades Advanced                           |
|---------------------------------------------------------------------------------|
| CPU:                                                                            |
|                                                                                 |
| Num of CPUs:      4                                                             |
|                                                                                 |
|       CPU        Used                                                          |
|         1          6%                                                          |
|         3          5%                                                          |
|         0          1%                                                          |
| ------------------------------------------------------------------------------ |
| Memory:                                                                         |
|                                                                                 |
|            Total MB   Used MB   Free MB                                        |
| Physical      1,958       827     1,131                                        |
| FW Kernel     1,567       194     1,372                                        |
| Swap          4,126         0     4,126                                        |
| ------------------------------------------------------------------------------ |
| Network:                                                                        |
|                                                                                 |
|- More info available by scrolling down -----------------------------------------|
```

CPView

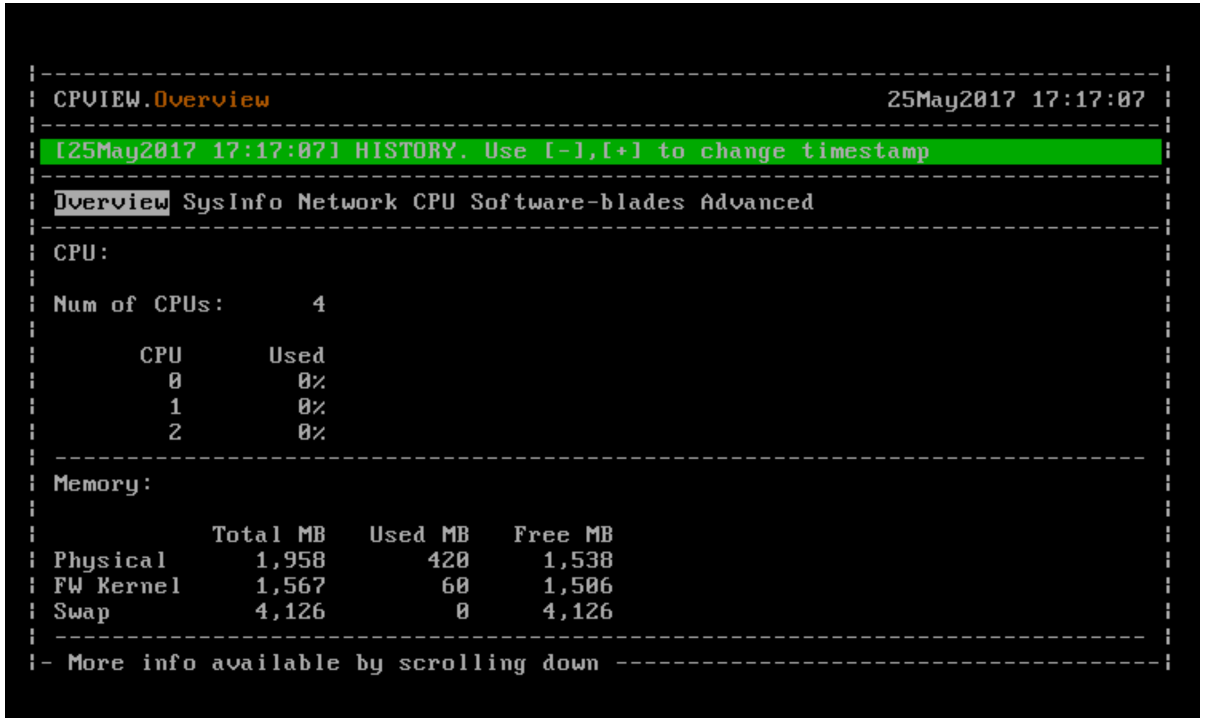
- Real Time Statistics
- No Overhead on CPU on most counters
- Sub Menus and Counters



```
|-----------------------------------------------------------------------------|
| CPVIEW.Network                                          02Jun2017 12:14:39 |
|-----------------------------------------------------------------------------|
| Overview SysInfo Network CPU Software-blades Advanced                       |
|-----------------------------------------------------------------------------|
| Traffic Interfaces Top-Protocols Top-Connections                            |
|-----------------------------------------------------------------------------|
| Traffic Rate:                                                               |
|                                                                             |
|                           Total          FW         PXL   SecureXL         |
| Inbound packets/sec          13          13           0          0         |
| Outbound packets/sec          8           8           0          0         |
| Inbound bits/sec         99,549      99,549           0          0         |
| Outbound bits/sec        51,987      51,987           0          0         |
| Connections/sec               0           0           0          0         |
| --------------------------------------------------------------------------- |
| Concurrent Connections:                                                     |
|                                                                             |
|                           Total          FW         PXL   SecureXL         |
| Connections                  20           8          12          0         |
| Non-TCP                      14           2          12         12         |
| TCP handshake                 0           0           0          0         |
| TCP established               6           6           0          0         |
|- More info available by scrolling down -------------------------------------|
```

CPView History

- Historical Data
- Per Minute performance statistics
- Option to view specific date
- Option to view specific time



```
|------------------------------------------------------------------------------|
| CPVIEW.Overview                                        25May2017 17:17:07 |
|------------------------------------------------------------------------------|
|[25May2017 17:17:07] HISTORY. Use [-],[+] to change timestamp                 |
|------------------------------------------------------------------------------|
| Overview SysInfo Network CPU Software-blades Advanced                        |
|------------------------------------------------------------------------------|
| CPU:                                                                         |
|                                                                              |
| Num of CPUs:       4                                                         |
|                                                                              |
|       CPU       Used                                                        |
|         0         0%                                                        |
|         1         0%                                                        |
|         2         0%                                                        |
| ---------------------------------------------------------------------------- |
| Memory:                                                                      |
|                                                                              |
|             Total MB    Used MB    Free MB                                   |
| Physical        1,958        420      1,538                                  |
| FW Kernel       1,567         60      1,506                                  |
| Swap            4,126          0      4,126                                  |
| ---------------------------------------------------------------------------- |
|- More info available by scrolling down --------------------------------------|
```

Summary

- Used Smart Event and event correlation
- Applied Smartview Monitor and real time monitoring
- Used CPView to monitor the Security Gateway real time performance and historical performance

Bibliography

Check Point R80.10 Logging and Monitoring Admin Guide California: USA

Check Point R80.10 CPView Guide California: USA