Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point Monitoring Software Blade

View a complete picture of network and security performance and alerts

Security Management

Monitoring Software Blade

THE CHALLENGE

Corporate networks in today's dynamic business environment are often comprised of many networks and gateways that support a diverse set of products and user needs. The challenge of managing an increasing array of system traffic can put enormous pressure on IT staffing capacity and network resources.

Security managers need a cost effective solution to obtain a complete picture of network and security performance. A high performance network and security analysis system would help security managers administer their networks by establishing work habits based on learned system resource patterns. An effective monitoring solution with a single, central interface would enable security managers to respond quickly and efficiently to changes in gateways, tunnels, remote users and traffic flow patterns or security activities.

OUR SOLUTION

The Check Point Monitoring Software Blade presents a complete picture of network and security performance, enabling fast responses to changes in traffic patterns or security events. The Software Blade centrally monitors Check Point devices and alerts security administrators to changes to gateways, endpoints, tunnels, remote users and security activities.

SmartView Monitor allows administrators to easily configure and monitor different aspects of network activities. Graphical views can easily be viewed from an integrated, intuitive interface.

Pre-defined views include the most frequently used traffic, the status of VPN tunnels, gateway system history, and remote user information. For example, Check Point system counters collect information on the status and activities of Check Point products (for example, firewall, VPN and IPS). Using custom or pre-defined views, administrators can drill down on the status of a specific gateway and/or a segment of traffic to identify top bandwidth hosts that may be affecting network performance. If suspicious activity is detected, administrators can immediately apply a firewall rule to the appropriate Security Gateway to block that activity. These firewall rules can be created dynamically via the graphical interface and be set to expire within a certain time period.

Real-time and historical graphical reports of monitored events provide a comprehensive view of security and performance over time.

PRODUCT FEATURES

- Real-time gateway status and utilization information
- Comprehensive network usage display
- Suspicious activity monitoring
- Customized alerts for automated notifications
- VPN tunnel status and connection data
- Remote user monitoring
- Flexible, graphical reporting
- Fully integrated into Software Blade Architecture & Management
- Activate monitoring on any Security Management server
- Supported on Check Point Appliances and open servers

PRODUCT BENEFITS

- Real-time information on Check Point products
- Monitor connectivity between gateways and remote user traffic
- Cooperative Enforcement® verifies connections from internal and remote hosts
- Detailed or summary graphs and charts for analysis of traffic patterns
- Automatically modify access privileges upon detection of suspicious activity
- Save time and reduce costs by leveraging existing security infrastructure

softwareblades™

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

CHECK POINT MONITORING SOFTWARE BLADE FEATURES

Gateway Monitoring
The Monitoring Software Blade provides real-time information on Check Point gateways in the organization. Custom and predefined queries enable administrators to view in-depth information, such as system data, network activity, policy and license status about specific gateways.

Network Traffic Monitoring
The Monitoring Software Blade also delivers a comprehensive view of network usage. It can generate detailed or summary graphs and charts for analysis of network traffic patterns, audit and estimate costs of network use, identify departments and users that generate the most traffic, and detect and monitor suspicious activity.

Suspicious Activity Monitoring and Alerts
The Monitoring Software Blade integrates the Check Point suspicious activity monitoring protocol for modifying access privileges upon detection of any suspicious network activity, such as attempts to gain unauthorized access. Alerts can also be automatically sent to administrators for certain predefined system events such as when free disk space is below an acceptable threshold or if a security policy has been changed. These alerts point to potential system security threats and provide information to assist in avoiding, minimizing or recovering from damage.

VPN Tunnel Monitoring
The Monitoring Software Blade enables system administrators to monitor connectivity between gateways. Permanent tunnels can be set up between Check Point gateways where uninterrupted connectivity is critical to the organization's business. By constantly monitoring the status of VPN tunnels, including inbound and outbound tunnel traffic, the Monitoring Software Blade enables administrators to track normal tunnel functions so that malfunctions and connectivity problems can be quickly resolved.

Remote User Monitoring
The monitoring of remote users offers valuable information for identifying and troubleshooting remote connectivity issues. The Monitoring Software Blade provides comprehensive information on various aspects of remote user traffic, such as current open sessions, overlapping sessions, route traffic and connection time.

Cooperative Enforcement Monitoring
The Cooperative Enforcement monitoring feature utilizes the endpoint security server compliance capability to verify connections arriving from internal and remote hosts across the network. The logs generated for authorized and unauthorized hosts can be monitored via the Monitoring Software Blade.

Flexible, Graphical Reporting
Using custom or predefined queries, administrators can drill down on a specific segment of traffic or specific gateways to isolate factors that may be affecting network performance. Multiple views can be displayed within the same window and viewed side-by-side to enable easy diagnoses of traffic or security problems.

Tight Integration with Check Point Products
The Monitoring Software Blade is part of Check Point Security Management solutions, a suite of powerful applications for centrally configuring, managing and monitoring Check Point perimeter, internal, Web and endpoint security gateways. This integration results in reduced complexity and lowers total cost of ownership.

Integrated into Check Point Software Blade Architecture
The Monitoring Software Blade is integrated into the Software Blade Architecture. It can be easily and rapidly activated on existing Check Point Appliances or open server platforms, saving time and reducing costs by leveraging existing security infrastructure.

Full integration into the modular Software Blade Architecture allows for rapid and easy activation on any Check Point Security Management server.

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

SOFTWARE BLADE SPECIFICATIONS

Feature	Detail
Secure Status Updates of Remote Modules	• Via Check Point OPSEC APIs like AMON
Customizable System Overview	Including: • Customize by gateway • Overall status • Average CPU • Memory • Disk free %
System Information	• OS, CPU, memory, hard disk free %, and network activity
Product Status Information	Including: • Firewall • VPN • ClusterXL • Antivirus
Customizable Threshold Settings	• Set actions globally or per gateway for when a threshold is met, e.g. when a remote gateway fails
Customizable Actions	• Log, alert, email, SNMP trap, and user- defined
Customizable Reporting	• Gateways, traffic, counters, tunnels, and remote users
Reset Users and Tunnels	• Control user activity
Apply Dynamic Enforcement Rule	• Per gateway, source, destination, and service
ClusterXL Member Control	• Start and stop the ClusterXL processes

CONTACT CHECK POINT

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

December 2, 2013