

# CHECK POINT + NXLog

## LOG COLLECTION SOLUTION



### CENTRAL LOG COLLECTION

#### Product Benefits

- Centralize your log collection with a solution that integrates with Check Point Next Generation Firewalls
- Retrieve real-time and historical security events to elevate your monitoring and incident response efforts
- Meet strict auditing and industry compliance requirements

### INSIGHTS

Gaps in logging and analysis of the network perimeter allows malicious actors to conduct reconnaissance, attack and then move laterally within networks.

Awareness of the network compromise may happen immediately, but is more likely to go undetected weeks and months after the initial breach. Regardless of the timeline, complete logging records detailing proof of these activities is a requirement whether it is through almost-real time monitoring or as part of an incidence response.

In the absence of a solid audit log solution that maintains the integrity of your logs, an attack may remain invisible. Even worse your logs may be cleaned or even destroyed damaging or delaying your incident response efforts.

Check Point and NXLog bridges these monitoring gaps. With sufficient logging - through the collection of security events from Check Point Next Generation Firewalls - not only will your security teams be able to monitor for network breaches, but it can also provide evidence of any successful attacks.

### CENTRALIZED LOG COLLECTION

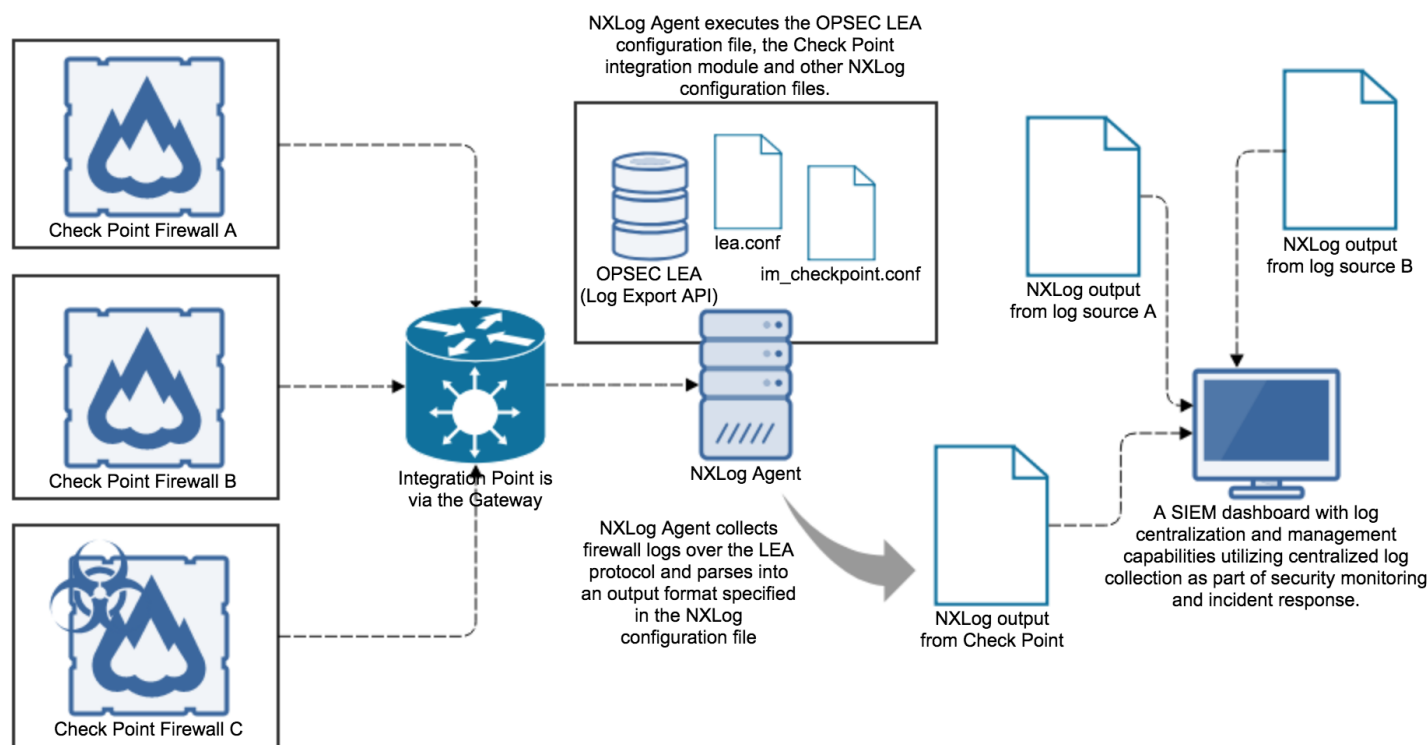
Check Point and NXLog have partnered to ensure you have a safe and reliable centralized log collection solution protecting your organization. By seamlessly integrating logs from Check Point Next Generation Firewalls, network and security administrators are prepared for the next attack with an efficient, centralized network and security monitoring solution.

Using the NXLog Enterprise Edition custom module for Check Point Next Generation Firewalls, administrators can configure the NXLog Agent to obtain logs from Check Point Firewalls over the OPSEC LEA protocol.

Once configured, Check Point Next Generation Firewalls can send logs to the NXLog Agent for log collection via the OPSEC LEA protocol. Finally, the logs can be used for further analysis and threat hunting using a SIEM suite and other unified security management solutions.

With a centralized log collection strategy in-place, your security specialists are able to work with security events from Check Point Next Generation Firewalls and logs from other devices and sources. This central log collection and aggregation elevates your ability to monitor and respond to security incidents.

## WELCOME TO THE FUTURE OF CYBER SECURITY



Analyzing logs from a number of firewalls can be an extensive and expensive effort, especially with manual examination. Therefore, once configured in NXLog, these logs can be further parsed into structured data format as part of the log collection process. This means that audit logs can become more useful - providing structured data format for inspection by skilled and intuitive security personnel as well as being fed into automated log analysis tools. Do not allow weak gaps in your network. Leverage the security expertise through the integrated solution offered by Check Point and NXLog - centralize your firewall log collection capability with the NXLog Check Point module.

## ABOUT CHECK POINT

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

## ABOUT NXLOG

NXLog Ltd. (<https://nxlog.co>) specializes in developing IT security tools including secure log collection solutions as the primary focus. With the NXLog Enterprise Edition, customers can build a secure, flexible and reliable log infrastructure which satisfies the highest IT requirements of any organization and enables them to achieve regulatory compliance, easily identify security risks and policy breaches or analyze operational problems. NXLog enterprise customers belong in a number of industry sectors such as financial, government, industrial/manufacturing, gaming, entertainment, health, education, retail, military/defense and more.

### CONTACT US

**Worldwide Headquarters** | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: [info@checkpoint.com](mailto:info@checkpoint.com)  
**U.S. Headquarters** | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2117 | Fax: 650-628-2117 | [www.checkpoint.com](http://www.checkpoint.com)