

CHECK POINT + NETFLOW AUDITOR

ULTIMATE NETWORK ANOMALY ANALYTICS AND FORENSICS

BENEFITS

- Provides an integrated performance management, capacity planning, and security monitoring environment
- Eliminate network blindspots
- Anomaly detection, security forensics and performance monitoring to highlight hidden anomalies
- Perpetual diagnostics detect spurious traffic from DDoS attacks, P2P abuse and insider threats
- End-Point threat intelligence identifies botnets, hackers, traders in illicit material, or other known bad actors
- Complete drilldown forensics into suspect communications
- Easy to deploy, easy to use
- Highly automated: requires a low labor effort to manage

INSIGHTS

The information security landscape has become so complex and diversified that companies need reliable and real-time diagnostics, network analysis and performance monitoring to leverage existing security strategies.

JOINT SOLUTION

Check Point and NetFlow Auditor have partnered to enable enterprises to have uncompromised protection against all types of threats and real-time qualification and granular historical visibility of all traffic flows recorded for enhanced security forensics, compliance, trending, alerting and automated traffic diagnostics.

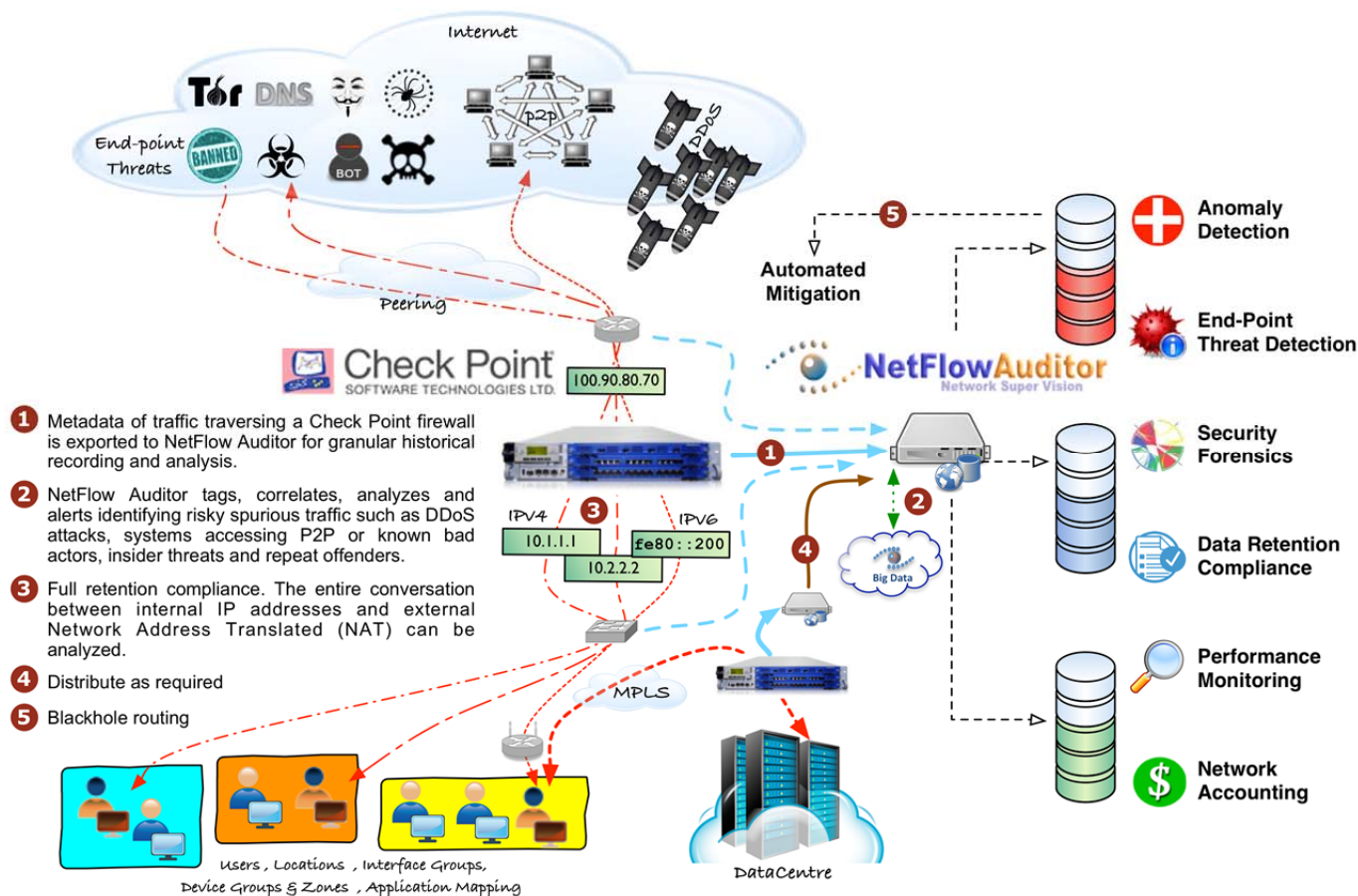
Check Point's fined-grained packet-based access control coupled with NetFlow Auditor's granular flow-based real-time detection and long-term security surveillance provide an enhanced security solution with complete visibility into suspect communications and connects the dots between internal IP addresses and external Network Address Translated (NAT) conversations substantially strengthening the ability to defend your digital assets.

A Check Point firewall is positioned at key points in a network to control access. Traffic metadata traversing the Check Point firewall is exported to NetFlow Auditor for granular recording and analysis.

NetFlow Auditor's intelligent agent technology analyzes flow records in real-time and uses machine learning making use of historical data trends and threat intelligence to identify risky spurious traffic such as DDoS attacks, P2P abuse and insider threats, and to mitigate security threats that would otherwise be hidden.

Auditor's measurements provide engineers clear analytics to completely understand their traffic flows enabling access lists to be more clearly checked or monitored when access has been discontinued enabling unnecessary rules to be removed maintaining Check Point firewall efficiency. IPv4, IPv6, MAC, QoS, MPLS, VLAN, ASN and application grouping and real-world naming make it easy to identify traffic ownership.

NetFlow Auditor constantly monitors your network traffic and provides total visibility to quickly identify and alert on who did what, where, when, with whom and for how long.



Authentication Flow Diagram

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is the largest pure-play security vendor globally that provides industry-leading solutions and protects customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices, in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes. At Check Point, we secure the future.

ABOUT NETFLOW AUDITOR

Since 1995 IdeaData has been a leader in supplying network analytics solutions for the Enterprise and ISP/Telco marketplace. IdeaData's NetFlow Auditor is a premier flow-analytics solution providing forensics, anomaly detection and extreme visibility eliminating network blindspots. Trusted globally by the largest companies for its comprehensive distributed traffic accounting for all flow types including Netflow, sFlow and IPFIX. NetFlow Auditor's granularity, scalability and flexibility helps organizations to reduce the risks associated with poor performance and security threats. For more information, visit www.netflowauditor.com.