CHECK POINT + FLOWMON NETWORKS SECURE AND EFFECTIVE IT INFRASTRUCTURE

Benefits

A secure and effective IT infrastructure solution provides customers with multilayered protection against common as well as sophisticated threats and ensures the customer's infrastructure is secure and stable. The key benefits of a secure and effective infrastructure are:

- Automated protection against common network perimeter threats
- Detection of threats on the Internal network as well at the perimeter
- Early detection of the indicators of threats leads to early prevention
- Prompt network problem troubleshooting thanks to detailed network visibility
- Regular network condition reports, options for network capacity planning
- Scalable and cost-effective architecture provides complex network protection
- Simplification and automation of time-consuming incident investigations
- Use existing network components as data sources such as Cisco, Enterasys, HP, Huawei, Mikrotik and Nortel
- Device outputs are integrated into a single dashboard

INSIGHTS

IT infrastructure complexity is on the increase as organizations adopt new products and incorporate new types of services. At the same time threats against computer networks are increasing in frequency and sophistication, overcoming traditional network security protections. Once hackers have bypassed the perimeter security and have established a beach hold in the corporate network, they often find security defenses if they exist are then easy to circumvent. With our increasing dependence on computer networks and information technologies, any breach can be devastating. Network outages are not only unpleasant to users. For companies who are now dependent upon ecommerce and customer trust that their data is secure, a data breach or network outage may lead to lost profits or even bankruptcy in the most severe cases. To provide the best protection against cyber threats a holistic approach that combines perimeter, endpoint and Local Area Network security and has visibility into what is happening in each area is needed.

SOLUTION

A secure and effective IT infrastructure occurs when network perimeter and internal network security solutions and network operational system controls are integrated.

Perimeter Security

The first step towards the creation of a safe infrastructure is deploying multilayered security protection at the perimeter. It is not sufficient to block undesirable traffic only by default firewall rules. To detect modern threats, deep packet inspection into the application level and of files is needed. A modern perimeter security solution must be able to identify and block tens of thousands of known versions of malicious software in real time and augment the with sandbox technology to find unknown and zero-day threats.

Network perimeter security is ensured with an industry-leading Next Generation Threat Prevention solution from Check Point. Detect and prevent external threats with NSS Recommended firewall and IPS. Prevent flood and application level DoS attacks with Check Point DDoS Protector. Educate and enforce employee use of the World Wide Web with Application Control and URL Filtering. Detect infected hosts with Anti-Bot. Prevent employees accidentally leaking sensitive documents with Data Loss Prevention. Inspect files for known malware with Antivirus and emulate unknown files in a virtual sandbox with the ThreatCloud Emulation Service. Send network perimeter traffic information from Check Point to Flowmon Networks FlowMon.

LAN Visibility

The second essential step is to monitor the local network for attacks which may have successfully bypassed the perimeter. These threats may be from internal users or may occur when an infected mobile laptop or USB device is connected to the local network. Following the initial compromise advanced threats are designed to evade detection so that they can do reconnaissance and freely spread laterally within the network, blending in with legitimate network traffic. Due to their covert operations they may be undetected for weeks and even months. Even though network perimeter security solutions are improving, it is now not a question of how to eliminate the possibility of the network attack, but how to detect such an attack as soon as possible. The FlowMon solution accepts perimeter information from Check Point and internal feeds from multiple other devices to give a holistic picture of network traffic. FlowMon supports Cisco standards NetFlow v5, NetFlow v9, NBAR2 and general protocols IPFIX or sflow; FlowMon probes are compatible with a wide range of network components. If the existing infrastructure does not support NetFlow, it’s possible to use a dedicated FlowMon Probe connected to core switches on the LAN. FlowMon Collector gathers, stores and processes NetFlow data so that it can subsequently be used for reporting, traffic analysis, troubleshooting of network problems and for network development planning.

LAN Security

Another important component in securing the network is thorough maintenance and full transparency of network operations across the infrastructure - facilitating prompt and efficient problem resolution, automated detection of operational problems and anomalies in network traffic. The FlowMon Anomaly Detection System (ADS), recognized by Gartner as one of the top solutions for advanced threat detection and network traffic monitoring, automates the detection of threats and anomalies in network traffic using Network Behavior Analysis (NBA) technology. Data is automatically processed in real-time, providing instant protection from threats. Network traffic history is available as evidence for a forensic analysis.

Endpoint Security

Sometimes threats manage to bypass network perimeter solutions or infect endpoints when they are off network. Check Point Endpoint Security is a comprehensive suite that includes firewall and anti-malware protection. Media Encryption provides centrally-enforceable encryption of removable storage media such as USB flash drives, backup hard drives, CDs and DVDs. Full Disk Encryption ensures your data is safe even when the mobile device is lost or stolen.

IN SUMMARY

A unique combination of Next Generation threat prevention from Check Point with the ability to automatically detect and eliminate threats at the network perimeter and on endpoints combined with the FlowMon solution for full-scale internal network visibility and automated threat detection represents an effective solution to protect one´s organization against advanced cyber threats and for establishing an effective and stable IT infrastructure. As a result implementation costs as well as network troubleshooting time are also reduced thanks to the integration of both solutions.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com), is the largest pure-play security vendor globally, 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 FLOWMON NETWORKS

Flowmon Networks empowers businesses to manage and secure their network infrastructure confidently. Through our high performance monitoring technology and lean-forward behavior analytics, IT pros worldwide benefit from absolute network traffic visibility to enhance network & application performance and deal with modern cyber threats. Driven by a passion for technology, we are leading the way of NetFlow/IPFIX network monitoring that is high performing, scalable and easy to use. Enterprises, internet service providers, government entities or even small and midsize companies rely on our solutions to take control over their networks, keep order and overcome uncertainty. Recognized by Gartner, Flowmon Networks is one of the fastest growing companies in the industry.