Secure and Effective IT Infrastructure

Purpose of this document

The IT infrastructure complexity is increasing in today´s modern world. New products are constantly being released as well as new types of services are being used. There is an ever rising threat to the security of computer networks. Sophisticated and targeted attacks being able to overcome the traditional computer network protection perimeter are at the very top of such threats. After having bypassed the security solutions such attacks infiltrate a corporate network, within such the possibilities of defense are extremely limited. In fact, the vast majority of organizations is currently getting evermore dependent on computer networks and information technologies. Getting a station infected, losing data or having to endure a several hours' network outage is an unpleasant as well as troublesome matter. A successful IT infrastructure attack or a long-term outage of the entire network can be of liquidating effects to a whole organization.

The document describes:

- Main challenges to the area of effective computer network management and full-scale protection against cyber threats
- Secure and effective IT infrastructure solutions

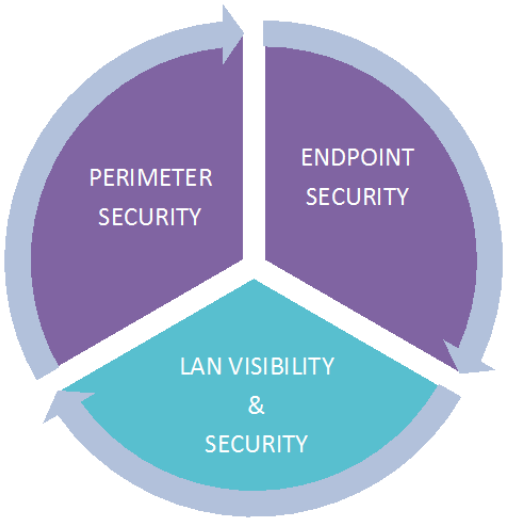

Figure 1: Full-scale network security technologies

Challenge

The first step to be made towards a safe infrastructure is network protection on its perimeter. It is not sufficient to block undesirable traffic only by default firewall rules. It is essential to detect modern threats, check passing data on the application level and disclose known malware and attacks in order to protect the internal network in the best way possible. A modern perimeter security solution must be able to identify and block tens of thousands of versions of malicious software in real time while continually updating the database of known threats in such a way that it is able to intercept as many new threats as possible and reduce the risk of sensitive organizational data leakage.

The second and essential step is monitoring the operation of a local network in such a way that attacks which successfully bypass the perimeter or are caused by internal network users themselves (employees, hosts who get access to the network) are dealt with. Advanced threats are made not to be easily identified and they are able to bypass the network perimeter protection or to find a different way of getting into the network, instead of having to surpass the perimeter in order to get there. After having done so they operate within the network and freely spread being considered legitimate by standard security tools. Thanks to their covert operations they are able to spy on sensitive data or people in the long-term. Even though the network perimeter security solutions are improving, it is now not a question of how to eliminate the possibility of the network being attacked, but how to detect such an attack as soon as possible. One of the best examples is an industrial espionage malware found in 2012. It was programmed to steal technical drawings and industrial designs and to send them to servers located in China. This malware is known as ACAD/Medre.A and it has supplied the servers in China with thousands of AutoCAD documents.

A very important predisposition for making the network secured is its thorough maintenance. Nowadays, it cannot be done without full-scale transparency of network operations across the infrastructure, prompt and efficient problem solving capacities, or automated detection of operational problems and anomalies in network traffic. Modern security solutions for an effective and secure network must become a tool not only for the network security department but also for the network department itself and must ensure a rapid and high-quality information exchange between the two above mentioned realms.

The last step is to check every single endpoint for undesirable software. That is why we use antivirus programs.

Solution

The desirable and effective IT infrastructure is a combination of the below mentioned elements of network perimeter and internal network security solutions and network operational system control:

- Network perimeter security is ensured by a cutting edge firewall by Check Point with abilities to automatically detect and block all known threats. It is also able to keep record of the communication on the network perimeter. Gartner, an analytic company, has considered Check Point a leader in the firewall business for 16 years.
- Internal network visibility by means of network traffic monitoring is performed by Flowmon solution supporting Cisco standards NetFlow v5, NetFlow v9, NBAR2 and general protocols IPFIX or sflow. The Flowmon solution can be applied to any clients´ infrastructure thanks to its own probes and compatibility with a wide range of network components.

- Automated detection of incidents in the internal network is done by the Flowmon ADS (Anomaly Detection System) solution which is a part of the Flowmon solution. The Flowmon ADS solution also operates with information about communication on the network perimeter sent by Check Point firewall in order to carry out a more accurate and effective threat analysis. The Flowmon solution is regularly identified in Gartner reports, which recognizes it as one of the top solutions for advanced threats detection and network traffic monitoring.
- Endpoint protection against common threats, which managed to surpass the network perimeter solutions or infected the endpoint in some other way, is performed by Check Point Endpoint Security. Check Point Endpoint Security also provides the possibility of endpoint and portable media ciphering as protection against data leakage in case of equipment loss.

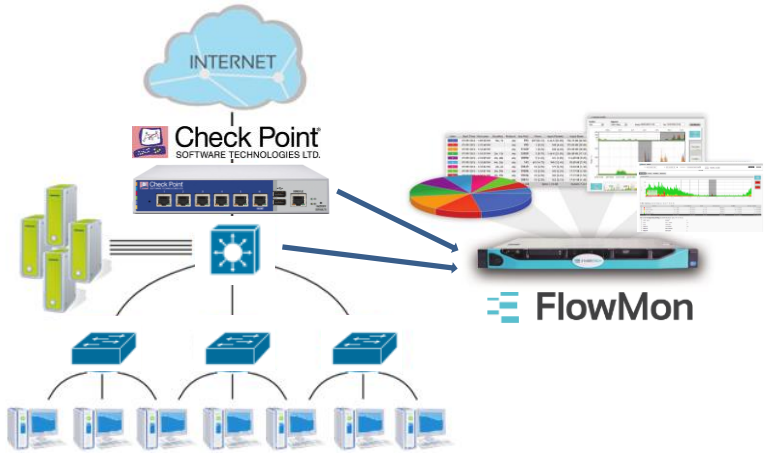

Figure 2: Solution components for network protection against advanced cyber threats

Thanks to this compact solution the customer is provided not only with protection against common threats on the network perimeter and at endpoints but also with the ability to intercept threats, which are active within the internal organization network. Detailed network traffic visibility provides the customer with a view of operational problems, anomalies in network traffic or suspicious behavior and activities which typically suggest a forthcoming attack. The Flowmon solution is also able to more easily identify the extent and importance of such a security incident thanks to being provided with additional information about the network perimeter traffic by Check Point firewall.

Solution benefits

Secure and effective IT infrastructure solution focuses on providing customers with complex network protection against common as well as sophisticated threats and ensuring the clients´ infrastructure is secure and stable. The key benefits of the solution for an effective and secure infrastructure are:

- Automated protection against common network perimeter threats
- Internal network threat detection in case these surpass security solutions
- Ability to intercept initial symptoms of threats and theirs 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 providing complex network protection
- Simplification and automatization of a time-consuming incident investigation

- Ability to use existing network components as data sources (Cisco, Enterasys, HP, Huawei, Mikrotik, Nortel and so on)
- Ability to integrate the outputs into a single dashboard

Solution components

Common threats detection on the network perimeter

The advanced Next Generation firewalls by Check Point contain specialized firewall solutions, which detect and prevent threats coming from the Internet (IPS modules, DDoS, Anti-virus, Anti-bot, Threat Emulation in a Virtual Environment), control and secure outgoing internal traffic (Application Control modules, URL Filtering, Anti-bot) and at the same time protect an organization against sensitive data leakage (DLP module). Thanks to these features the Next Generation firewalls are able to detect any undesirable traffic on the network perimeter without the necessity of being launch by staff and that is how they significantly increase the security of the network on its perimeter.

Check Point firewalls are also used to generate information about network perimeter traffic for the Flowmon solution.

Generating, recording and NetFlow data analysis to ensure full-scale network traffic visibility

Generating information about the internal network traffic of a customer is ensured by existing active network components. In case the existing infrastructure does not allow NetFlow to generate data, it is possible to use a dedicated Flowmon Probe connected to LAN core switches. Check Point firewall generates NetFlow on the perimeter. In this way it is possible to file information about every realized connection in the network.

NetFlow gathering, storage and processing is provided by the Flowmon Collector by Flowmon Networks. Thanks to the Flowmon solution the information can be subsequently used for reporting, for traffic analysis, for troubleshooting of network problems or for network development planning. The Flowmon Collector is able to acquire NetFlow from a wide range of network components, for example from Check Point firewalls, and offers full-scale network traffic visibility.

Automated detection of threats and suspicious behavior within the internal network

Automated detection of threats and anomalies in network traffic is performed by the Flowmon ADS (Anomaly Detection System) by Flowmon Networks based on Network Behavior Analysis (NBA) technology. It is a security enhancement of a Flowmon Collector which uses collected network traffic data. These data are automatically processed in real-time and it provides us with a possibility of instantaneous protection against threats on the way. It also allows us to save network traffic history in the long-term and provides us with so much needed evidence or records for a forensic analysis carried out even a few years retroactively.

Why solutions for a secure and effective IT infrastructure?

A unique combination of Next Generation firewalls by Check Point with the ability to automatically detect and eliminate threats on the network perimeter and the Flowmon solution for full-scale internal network visibility and automated threats detection system represents an effective way of protecting one´s organization against advanced cyber threats and of establishing an effective and stable IT infrastructure. As a result implementation costs as well as network troubleshooting time are being reduced thanks to the interconnection of both solutions.

More information

For more information, please contact your Check Point or Flowmon Networks partner.

Check Point Worldwide Headquarters
5 Ha'Solelim Street
Tel Aviv 67897
Israel
www.checkpoint.com

Flowmon Networks, a.s.
U Vodarny 2965/2
616 00 Brno
Czech Republic
www.flowmon.com