Securing the Security Provider

OVERVIEW

Industry

IT Consulting / Business Services

Key Requirements

- Assure privacy requirements in a multi-tenant environment
- Real-time forensic investigation
- Optimize bandwidth usage and improve capacity planning

Solution

ManageEngine Firewall Analyzer

Results

- Instant notification for anomalous network activities and archival of logs for forensics
- Bandwidth analysis reports provides insights into firewall
- Specific bandwidth usage trends and optimize network capacity

The Customer

LCM Security is a managed security services provider. LCM serves to improve security, ease compliance and optimize the performance of networks. LCM Security's methodology results in a secure, operationally effective environment that mitigates risk and successfully aligns business and security goals.

The Expectations of a Security Provider

Maximizing network and data security in the best interest of the clients – this is what LCM Security is all about. Though the task is described in mere six words on paper, it is an almost insurmountable task when considering the vulnerabilities involved. LCM Security provided security solutions bundled with a suitable firewall monitoring program and offered to monitor and report the network activities and anomalies of its clients.

Now came the bigger task of "securing the security provider": LCM Security had the need to monitor IPS events and study the pattern of the generated events. This demanded collecting network-activity logs over a period of time, and neatly classifying them in an easily retrievable pattern. Since the data is collected from multiple clients, privacy of information has to be assured at any cost. The data so collected is extremely sensitive and there cannot be a compromise on either speed or accuracy or security, favoring the other two. Parallel to IPS Analysis, LCM also needed reports on bandwidth usage patterns and data that would give a forensic insight in to their network and the activities.

With these many conditions to satisfy, LCM Security tried on many tools that could present a solution to effectively address all these concerns.

Enter Firewall Analyzer

Their search zeroed in on ManageEngine Firewall Analyzer: a web based tool for bandwidth monitoring and security reporting. It performs change management, configuration analysis and security audit of Firewall devices. Firewall Analyzer touted features that would make it an ideal choice for LCM Security.

> "Pulling information is a very quick process, particularly when doing a forensic analysis on the network."
>
> **Ken Muir,** Director of Information Security, LCM Security

Easy-To-Use Web-Interface meant a hassle-free adapting to the product's controls and functions. This also implies that Firewall Analyzer could be accessed almost from anywhere with appropriate credentials and it works on both platforms. The easy-to-navigate interface ensured that the required was available or at the worst, generated swiftly within a few clicks.

"...reasonably priced, very easy to use and has all the functionalities that we need". **Ken Muir**, Director of Information Security, LCM Security

The Ability to Drill-Down Information Granular information could be retrieved from Firewall Analyzer, so the exact event that led to some anomaly can be pin-pointed. This feature helped from a security-perspective and served to isolate the exact cause of network disruptions - LCM Security could lock on the infection-point in the network and the same could be mitigated. Firewall Analyzer also provided the IT Personnel in LCM Security in generating reports for users who logged in using SSL VPN. Vital reports like these can be obtained using Firewall Analyzer"s advanced search.

The fine detail of information in Firewall Analyzer's reports does not mean any delay – all Firewall Analyzer reports are generated in a jiffy.

The Support for Multiple Firewalls made Firewall Analyzer a one-stop solution for a company like LCM Security, which handled multiple firewalls. With Firewall Analyzer supporting Juniper, Fortinet, Cisco and a couple of dozen other popular firewalls, the need for using multiple tools for each kind of firewall was totally eliminated.

The Capacity to Analyze Trends: Firewall Analyzer's data proved useful for LCM to analyze the trends of attacks. The statistics drawn from Firewall Analyzer's reports helped them arrive at a monthly data for attacks on the network, and consequently served to measure the effectiveness of the counter-measures deployed to thwart the dangers of any malicious activity from within or outside the network.

With the granularity levels that Firewall Analyzer provided, LCM could also analyze malicious attacks on the network with respect to a specific port and also its targets. This aspect provided LCM with the much-needed insight to future threat-proof the network.

Firewall Analyzer's network traffic analysis also provides LCM with traffic trends over a period of time. LCM Security used this data to compare data gathered over a specific time period, and the inference was useful in optimizing their bandwidth resources and also for future capacity planning.

Key Results

All these features gave Firewall Analyzer gave that edge against the competitors which failed to give a wholesome solution. This made LCM Security deploy ManageEngine Firewall Analyzer and it was no surprise for them that they reaped a lot of benefits from there on. LCM Security saw a visible shift on their operating costs and security of their networks, all on the favorable end. Firewall Analyzer posed as the deterrent that would keep any undesirable eventualities at bay! To this day, Firewall Analyzer continues to be the preferred firewall-security management tool for LCM Security..

About ManageEngine Firewall Analyzer

ManageEngine Firewall Analyzer is an automated firewall log analysis tool for security event management that collects, analyses, and reports on enterprise-wide firewalls, proxy servers, VPNs, IDS/IPS, and other network perimeter devices. More than 3000 customers worldwide are using Firewall Analyzer as their Security Event Management solution to detect network anomalies, monitor firewall configuration changes (firewall change management), fine-tune firewall rules, measure bandwidth usage, manage user/employee internet access, audit traffic, and improve incident response.

https://forums.fwanalyzer.com www.facebook.com/LogAnalyzer https://twitter.com/LogGuru

About ManageEngine

ManageEngine is the leading provider of cost-effective enterprise IT management software and the only one making the 90-10 promise - to provide 90 percent of the capabilities offered by the Big 4 at just 10 percent of the price. More than 50,000 organizations in 200 countries, from different verticals, industries and sizes use ManageEngine to take care of their IT management needs cost effectively. ManageEngine is a division of Zoho Corp.

ManageEngine is a trademark of ZOHO Corporation. All other brand names and product names are trademarks or registered trademarks of their respective companies.