Firewall Analyzer helps Collabera to Gain Complete Visibility into their Client's Network Security Infrastructure

OVERVIEW

Industry

Information Technology and Services

Key Requirements

- Monitoring multiple firewalls in a multi-vendor environment
- Monitor Network bandwidth utilization
- Generate network security reports automatically
- Manage firewall configuration changes
- Get alerted when anomalous activities happen on their clients network

Solution

ManageEngine Firewall Analyzer

Results

- Centralized management and monitoring of all types of firewalls
- Bandwidth analysis reports are now generated automatically at pre-defined intervals
- Network security reports are generated automatically as per the defined schedule
- All configuration changes made to the firewalls get tracked with Firewall change management reports
- Alerts are sent in real-time via sms, email or custom program when anomalous activities happen on their client's network

The Customer

Collabera is a fast growing, end-to-end information technology services and solutions provider working with leading Global 2000 organizations from the Financial Services, Communications, Media, Manufacturing, Retail, Energy and Utilities domains. Collabera delivers highly responsive and innovative solutions that help clients align their IT strategy with business goals to address the most important IT needs. Collabera delivers a full portfolio of services that include IT Consulting, Application Development and Management, Independent Testing, Infrastructure Management Services, Enterprise Software Solutions, Business Intelligence & Data Warehousing as well as Professional Services.

Challenges

As a managed security services provider (MSSP), Collabera was responsible for defending its client's network against information security risks. Girish Ramachandran, Network Security Manager at Collabera faced several network security challenges while managing his client's network. It was becoming extremely difficult for Collabera in managing multiple firewalls in a multi-vendor environment.

Girish Ramachandran and his team used to manually monitor and analyze the firewall traffic logs from their client's firewalls. Identifying network issues or security threats from the terabytes of logs generated by their clients network security devices was like looking for a needle in a haystack!. "Monitoring such large and complex network security infrastructure manually was extremely time consuming and cumbersome" says Girish Ramachandran.

Collabera had to submit traffic and security audit reports to their clients pertaining to bandwidth usage, firewall change management, capacity planning and security threats - network hacker attacks, virus attacks, etc. Clients used to request for multiple reports on a daily/weekly/monthly basis and it was a tedious task to meet the requirements of their clients in a timely manner.

Monitoring the incoming and outgoing network traffic through the firewalls was also very complex without automated bandwidth monitoring tools. Keeping the clients network free from congestion was a challenge for Collabera. Manually monitoring the network traffic and preparing the bandwidth monitoring reports was never an easy task for Collabera. "We needed an automated bandwidth monitoring tool to monitor the networktraffic and generate bandwidth reports by analyzing the logs from our clients firewall environment" says Girish Ramachandran.

> " Managing a multi-vendor firewall environment is not at all complex now. Firewall Analyzer allows us to centrally manage and monitor all firewalls such as Juniper, Fortinet, Cisco and other popular firewalls "
>
> **Girish Ramachandran,**
> Network Security Manager, Collabera.

Majority of Collabera's clients needed to comply with ISO 27001 and PCI-DSS network compliance audits. Manually analyzing the firewall logs and preparing compliance audit reports was not a feasible option. Collabera wanted to automate the process of generating the firewall compliance audit reports for their client's network infrastructure.

Also, there were multiple users from their client organizations who were configuring and managing the firewalls. Keeping a track of all the changes done to the firewall configurations manually was impossible. Collabera required an automated firewall change management monitoring solution that would help them in tracking all the changes done on their client's firewall configurations.

Collabera needed a firewall log monitoring and configuration management solution that could provide complete visibility into their client's security infrastructure and automate the process of generating security audit reports.

Solution

ManageEngine® Firewall Analyzer

Collabera selected **ManageEngine Firewall Analyzer** to manage and monitor their client's network security devices. Firewall Analyzer enabled Grish Ramachandran's team to monitor client's firewalls and generate security reports easily. "Managing a multi-vendor firewall environment is not at all complex now. Firewall Analyzer allows us to centrally manage and monitor all firewalls such as Juniper, Fortinet, Cisco and other popular firewalls " mentions Girish Ramachandran.

Girish Ramachandran narrated one instance when one of his clients asked him whether he could provide them with firewall security reports using the log data of last 6 months. Girish Ramachandran was very thrilled to know that Firewall Analyzer could retrieve historical raw log data from any period of time and allowed them to conduct log forensics and generate security reports immediately.

Using Firewall Analyzer, Collabera could easily identify and analyze their client's network security problems. The log search feature empowered Girish and his team to run a simple log search and drill down into the raw firewall logs and pinpoint the exact log entry for the security incident.

Girish Ramachandran and his team now generate network security and compliance reports in minutes. Collabera's clients who require ISO 27001 and PCI DSS compliance accreditation are really impressed with the compliance reports generated by Firewall Analyzer. "Our clients do not have to wait for weeks or months to get their security and compliance reports. With Firewall Analyzer, the reports are generated automatically. I schedule the reports in Firewall Analyzer and get them straight into my inbox as per the defined scheduled" says Girish.

Firewall Analyzer monitored the incoming and outgoing network traffic by analyzing the logs received from each network interface of their client's Firewall devices and generated bandwidth reports that gave precise details such as which user, protocol group; network activity is consuming the bandwidth. Girish and his team now receive alerts in real-time when sudden spikes in bandwidth occurs thereby allowing them to take instant remedial action for managing their clients network traffic and bandwidth.

Firewall Analyzer's configuration change monitoring and management gave precise information on 'who' made 'what' changes, 'when' and 'why' to clients firewall configuration in real-time. Alerts are sent via SMS or email to Girish Ramachandran and his team members in real-time when any change occurs on their clients firewall.

The implementation of Firewall Analyzer has not only enabled Collabera to gain in-depth visibility into their clients firewall environment, but also enhanced its network security services and improved the quality of service delivered to its clients.

- -

About ManageEngine Firewall Analyzer

ManageEngine Firewall Analyzer is an agent-less Log Analytics and Configuration Management Software for network security devices. More than 3000 customers worldwide are using Firewall Analyzer for end-point security monitoring & analysis, change management, employee internet monitoring, bandwidth monitoring, capacity planning, policy enforcement, security & compliance audit reporting. Firewall Analyzer is vendor-agnostic and supports almost all open source and commercial network firewalls, IDS/IPS, VPNs, Proxies and related security devices. For more information on ManageEngine Firewall Analyzer, please visit http://www.fwanalyzer.com/.

http://blogs.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.

http://blogs.manageengine.com   www.facebook.com/manageengine   https://twitter.com/manageengine