ManageEngine
Firewall Analyzer

ME
Success Stories

Thunder Bay District Health Unit uses ManageEngine® Firewall Analyzer for Live Traffic Monitoring and Network Anomaly Detection

OVERVIEW

Industry

Healthcare

Key Requirements

- Real-time (Live) network & Internet traffic monitoring
- Instant alerts for security breaches
- Detailed network forensic reports

Solution

ManageEngine Firewall Analyzer

Results

- Log and SNMP-based Live Traffic reports provide real-time visual representation of the traffic load across network links
- Anomaly alerts provide instant notification for abnormal network events recorded by the firewalls
- Secure and tamper-proof log archives; powerful search engine to search on both the raw and formatted logs and instantly generate forensic reports from search results

The Customer

Thunder Bay District Health Unit (TBDHU) is a not-for-profit public healthcare agency operating in the Province of Ontario, Canada. TBDHU is in fact 1 of 36 other Public Health Units operating in the province of Ontario with over 200+ employees, they handle huge volumes of health-related data of general public over their network.

Challenges

TBDHU's Information Systems team were looking for a firewall monitoring software, that can:

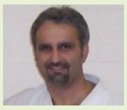
- Provide Live (real-time) reports of their Internet traffic
- Monitor Internet bandwidth utilization and alert them on sudden bandwidth jumps
- Generate instant alerts and detailed reports on network attacks, spyware, virus, port blocks due to attempted attacks
- Conduct firewall log forensics and provide detailed reports

Solution

ManageEngine® Firewall Analyzer

TBDHU's Information System's (IS) team were looking for a firewall traffic monitoring solution, to monitor their SonicWALL firewalls. A simple online search for an easy-to-use, robust firewall monitoring and reporting solution led them to ManageEngine Firewall Analyzer.

> “The implementation was so easy and the Firewall Analyzer immediately started showing me how much inbound and outbound traffic was passing through our firewalls. I now use Firewall Analyzer daily!”



Phil Avella,
Manager Information Systems, TBDHU

This software is used for end-point security monitoring & analysis, change management, employee Internet monitoring, bandwidth monitoring, capacity planning, policy enforcement, security & compliance audit reporting. Being agentless log analytics and configuration management software for network security devices, TBDHU Information Systems team could deploy, monitor and generate firewall traffic and security reports using Firewall Analyzer within minutes!

They were receiving useful and important insights on their network traffic like, Internet bandwidth utilization, top used and unused firewall rules, top attackers, top viruses and worms that have affected the network.

"The Live Reports available in Firewall Analyzer helps me monitor the Network and Internet traffic all day long and notifies us about any sudden jumps or dips in traffic. The software allows us to better manage not only our Internet connection but also our Firewalls too " said Phil.

"There were few instances where Firewall Analyzer helped us pinpoint security breaches, and we were able to immediately respond to such security threats and fix them," mentioned Phil. Firewall Analyzer continuously monitors the traffic flowing through TBDHU's network firewalls and looks out for abnormal network events which identifies viruses, attacks or security breaches. The software alerts the IS Team for any such network anomalies and provides them with detailed reports on the viruses active on the network, the hosts that have been affected, top attackers, top targets, protocols used for the attack, top denied hosts, denied protocols, and top security events generated.

TBDHU's IS Team often use Firewall Analyzer for their forensic investigations on past network activities, and detect any historical trends/patterns. Firewall Analyzer archives the logs received from their firewalls at pre-determined intervals, and these archived log files are then encrypted, hashed, and time-stamped to make them tamper proof. During forensic investigations the IS Team loads these archived files into the database and use Firewall Analyzer's powerful search engine to search the archived logs for anomalous events/patterns and generate forensic reports based on the search results.

"It is a fantastic product backed up by a responsive support team," says Phil Avella, who goes on to add "Obviously I had no idea how great the support would be until I experienced it first hand, right from the day I started evaluating Firewall Analyzer. Support is one of the things that I will continue to bring forward whenever I recommend your product."

About ManageEngine Firewall Analyzer

ManageEngine Firewall Analyzer is a web-based tool for change management, configuration analysis, security audit of firewall devices, bandwidth monitoring and security reporting. The software collects, analyzes and archives logs from network perimeter security devices and generates forensic reports. The devices supported include network firewalls, proxy servers, intrusion detection systems (IDS)/intrusion prevention systems (IPS) and virtual private networks (VPNs). The salient features of the application are firewall device management, bandwidth monitoring and security reports. 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 delivers the real-time IT management tools that empower an IT team to meet an organization's need for real-time services and support. Worldwide, more than 60,000 established and emerging enterprises — including more than 60 percent of the Fortune 500 — rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with offices worldwide, including the United States, United Kingdom, India, Japan and China.

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