

Stonylake Firewall Reporter: Anomaly Detection



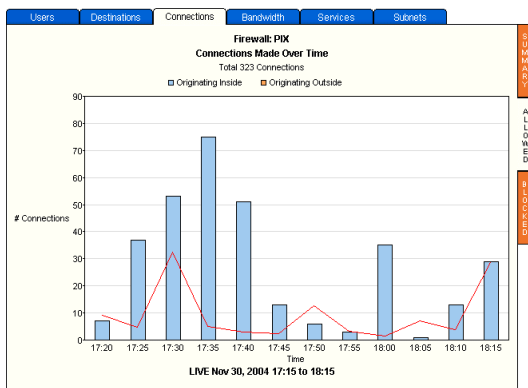
The Anomaly Detection System monitors and compares current firewall usage to historical moving averages in real time and emails alerts containing numerical values and a graphical snapshot of the trailing one-hour statistics when user specified pre-set thresholds are exceeded.

The Concept

Stonylake Firewall Reporter stores information logged by the firewall into a database after converting it to a consolidated format. The stored data provides trend patterns on firewall usage. This trend data is used to detect anomalies in actual usage.

How it works

The Administrator is required to set up as many monitoring rules as required. For every rule that is set up, the system calculates a moving average for each weekday. Current usage values are then compared continuously in real time with the corresponding average. Whenever the current values exceed the average values by a set percentage, an alert is sent out by the system. The email alert contains numerical values as well as a graphical snapshot of the trailing one-hour statistics and the moving average.



Usage

The Anomaly Detection System can be useful in many situations. For example:

- Bandwidth on SMTP. An alert could indicate a compromised email server or host.
- Bandwidth on FTP.
- Attempts and Connections on all services and all hosts. An alert could indicate an attack or serve as an early warning of an outbreak of a new virus.
- Connections or Attempts to a specific host e.g. a financial server
- Connections on a group of services used by trojans

System Requirements

Single application-database server configuration:

1.5GHz CPU, 768 MB RAM, 5.0 GB free hard drive space. Windows XP/Windows 2000 or RH Linux 9.0.

Dedicated application-database servers configuration:

Application Server: 1.5GHz CPU, 512 MB RAM, 1 GB free hard drive space.

Database Server: 1.5GHz CPU, 512 MB RAM, 5.0 GB free hard drive space.

Operating System: Windows XP/Windows 2000 or RH Linux 9.0.

Database: MS SQL Server 2000 or PostgreSQL 7.x