PAESSLER

WHITE PAPER

Network Monitoring as an essential component of IT security

White Paper

PRTG NETWORK MONITOR

Author: Daniel Zobel, Head of Software Development, Paessler AG
Published: July 2013

Contents

Introduction

According to a survey by Paessler AG, companies want to increase their protection against cyber threats and other damage in the future. Approximately 1,200 users were asked about the application of Paessler's software PRTG Network Monitor. The results of the survey show that 75% of these users find the tool to be an important security component for their networks. This white paper highlights the role that network monitoring plays as a supplemental security component in company networks, where challenges may arise and how these can be resolved.

Current Situation

IT SECURITY ACROSS THE GLOBE

Studies on IT security show that companies have some work to do in applying preventative security measures. Furthermore, cyber criminals are constantly developing more intelligent digital threats, which can be released in various ways.

A 2013 study by 41st Parameter found that two-thirds of Internet users have been victims of cybercrime, with more than 1.5 million new victims every day.

The use of mobile devices poses a major threat to corporate IT Security. According to The Trusted Mobility Index, a survey of 4,000 participants from the U.S., U.K., Germany, China and Japan, 41% of respondents using a personal device for work are doing so without permission of their employer, and one-third of IT professionals said their company had already experienced a mobile-related security threat.

According to figures from the Ponemon Institute, security breaches cost businesses $7.2 million per incident on average, a number that has climbed steadily over the past few years. About 85% of all U.S. companies have experienced one or more data breaches, and of those, more than one-third still have no formal process to handle the next breach.

By some estimates, the global damage caused by cybercrime could be as high as $1 trillion. That's why companies today should place a much higher priority on the importance of securing their IT infrastructure.

PROTECT IT SYSTEMS

Many companies assume their IT infrastructure is sufficiently protected by a reliable firewall and an up-to-date virus scanner. However, cyber criminals are developing more sophisticated methods of accessing company computers and servers. Security programs sometimes only recognize released Trojans, worms, etc. after it's already too late. As soon as the threat has access to one computer in the company network, it's usually just a matter of time before the entire system has been compromised.

The result is often data manipulation and loss, or takeover of computing capacity for criminal purposes. If the company-internal systems malfunction because of the malware attack, neither business communication between company locations, nor order processing, nor customer communication will function. The administrator is confronted with a time-consuming search for the exact source of the problem. Which components of the security system have failed? Which areas or components have been attacked by malware? Could there be other reasons why single systems have crashed?

In order to avoid such incidents, the complete IT infrastructure should be protected.

To this end, companies need a comprehensive IT security approach. In addition to firewalls and virus scanners, other measures such as encoding software, data security software, content filters, port scanners and other tools should be part of these systems.

Furthermore, in order to guarantee complete network protection, network monitoring should not be left out as a supplementary security measure. Targeted application of this type of solution can significantly raise the level of security in the IT environment.

Early Warning System in the Network

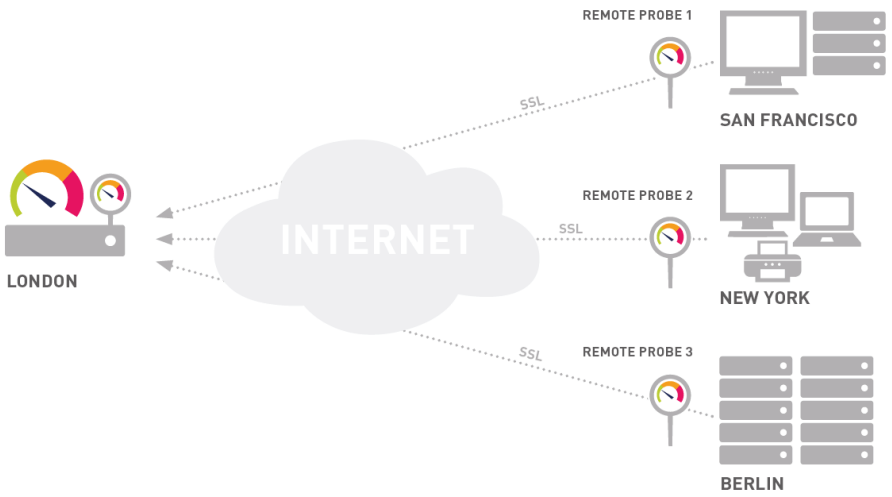
A network monitoring system generally serves to keep track of the entire IT infrastructure with all devices and systems. Administrators can monitor everything that uses a defined interface and delivers status information via standard protocol. The monitoring software must simply establish contact with the device or service using an IP address and can then retrieve the current device status.

This enables the IT department to keep an eye on the status of every area in the IT infrastructure at all times. The goal is to achieve maximum availability and optimum performance in the network. To do this, the network monitoring system must cover three security-relevant aspects:

- monitoring the actual security systems,
- identifying unusual occurrences, and
- checking environmental parameters.

Companies with multiple locations can use ‘remote probes’ to maintain centralized control of all three categories. A ‘probe’ is a small software program that monitors a remote network from within and sends the monitoring data to the central data server. In this way, a good network monitoring software monitors any number of network components, both in the main network as well as in the individual branches of the company. Components called ‘sensors’ are configured to monitor various parameters on the network devices and connections. In this way, the administrator has the entire network in view from a central location.

FIGURE:
Monitoring multiple locations with „remote probes“



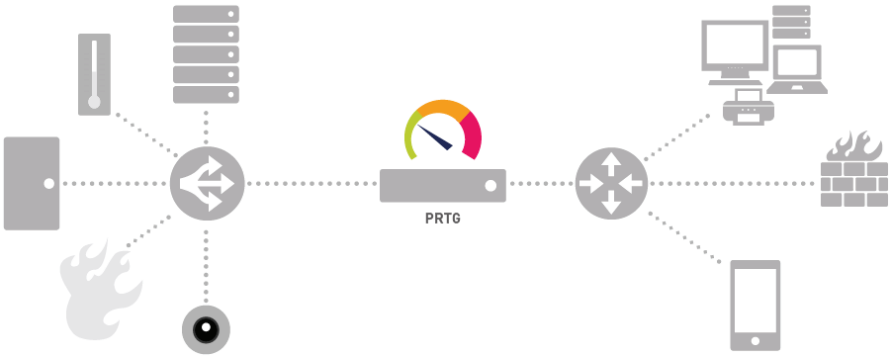
If the monitoring software notices a failure or unusual occurrence, it automatically sends an alarm to the responsible system administrator via text message or email. In this way, administrators are always immediately informed of any incidents, regardless of their location, and can react quickly.

The monitoring solution's early warning system is based on relevant, defined threshold values. If these are exceeded, the software sounds an alarm. The administrator is able to maintain permanent connection to the monitoring solution via web interface or smartphone app and can check any alarms immediately. He can then analyze the extent and severity of the issue and take appropriate action according to the live data from the monitoring.

Monitoring Security Aspects

IT administrators need to be able to react just as quickly to potential malware attacks. If installed antivirus solutions and firewalls don't discover attacks in time, the damage done can bring all operations to a standstill. By that time, administrators are only able to react to the problems, instead of being able to take proactive measures to prevent problems before they occur. The fact is that firewalls and virus scanners are not always sufficient on their own to guarantee all-around security for the network. Companies that integrate a network monitoring solution in their security strategy are able to discover potential dangers to the company network at early stages.

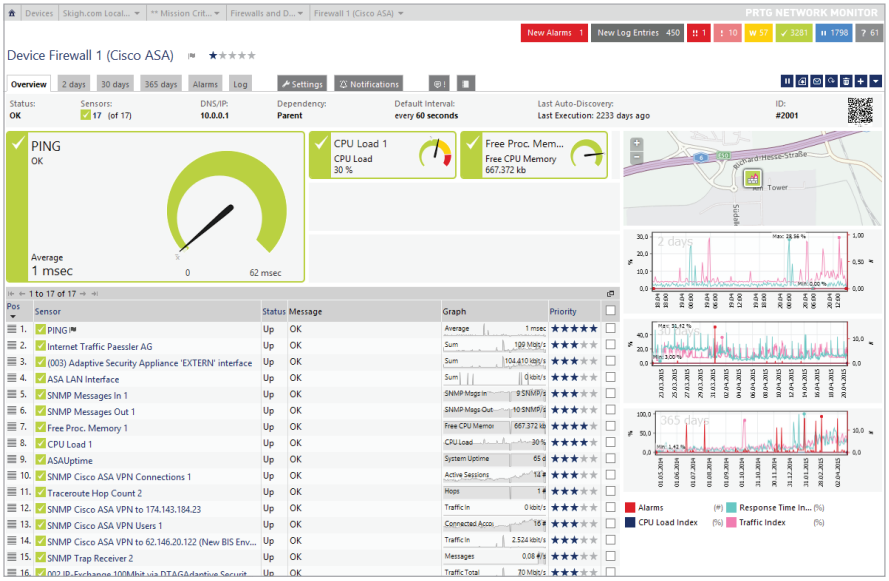
FIGURE:
Guaranteeing all-around security for the network



REGULARLY SCAN FIRE-WALLS AND VIRUS SCANNERS

An important task for the network monitoring solution is to check existing security systems, such as firewalls and virus scanners, for operational reliability. For example, the monitoring solution gathers detailed data regarding the performance and status of the firewall around the clock. If the firewall is not working properly, the risk of a malware attack on the network increases.

FIGURE:
The software monitors the status of the firewall



These malicious attacks could have the following effects: the CPU starts programs randomly or ports that should be closed are opened. To avoid this, administrators are informed of abnormalities in the firewall early on. The monitoring software can also check virus scanners running on the central mail server, for example. This helps companies to make sure that the scanner is constantly active. The monitoring solution uses special sensors to check the Windows Security Center to determine, for example, whether the virus scanners and anti-malware programs on each computer within the company are up-to-date and running seamlessly. This guarantees that client computers are continuously protected against malware as well.

BANDWIDTH BOTTLENECKS AS PROBLEM INDICATOR

Network monitoring solutions help administrators measure bandwidth for leased lines, network connections, devices (routers, switches), etc. Detailed monitoring of bandwidth usage can also indirectly detect malware attacks. An indication of an attack may be slow response times from applications and websites, caused by a malware program that takes up a lot of the bandwidth. In order to detect these inconsistencies, the monitoring software monitors various IP addresses, port numbers, protocols, etc. via packet sniffing or flow sensors. These flow sensors collect sent data and send them to the monitoring software for evaluation. The administrator can analyze the data and recognize problems early on, and initiate steps to remove the problem.

This type of bandwidth monitoring is especially suitable for networks with high data traffic. Unusual influences or activities—for example, malware attacks—can be recognized if the bandwidth usage exceeds defined thresholds or differs greatly from average values and usual fluctuation. In this case, the administrator can use the monitoring software to check which IP address, connection or protocol is using the most bandwidth and react accordingly.

MONITORING PHYSICAL ENVIRONMENT PARAMETERS

Last but not least, monitoring contributes to building security as well, as it enables surveillance of influences in the environment and surrounding area. Special devices with sensors for smoke or gas formation report fires or similar events at an early stage. In addition, sensors in the building can be configured in such a way that they trigger an alarm as soon as doors, windows or server cabinets are unlocked. IT administrators can even measure voltage using appropriate hardware and can transfer these data to the network monitoring software, which in turn identifies fluctuations in the power supply and notifies the administrators accordingly. Due to the many monitoring options, the IT team always knows whether the network is running in a safe environment or if short-, mid- or long-term changes must be made.

Analyzing Results

High-quality network monitoring solutions chart the entire monitoring data in reports and concentrate them into graphs or dashboards as well. The software consolidates the identified values of each component and system into easy-to-read reports. Not only are firewall and virus scanner activity sent to the administrator in a report but also service parameters, including current CPU and RAM usage of all servers and computers.

In addition, the availability of all network devices is visible for the IT department. The report even includes significant trends regarding network and bandwidth usage. If necessary, the administrator can draw comparisons between current and historical data for various situations. Current values that are worse than historical values show a definite need for optimization. Administrators can discover similar behavior between various sensors via automatic analysis of monitoring data and can thus identify previously unknown relationships between individual network components. Analyses of historical data, as well as identification of sensors with similar behavior patterns, are especially helpful for comparison studies in complex networks, in order to study the exact network usage levels and type of usage, and to close potential security gaps.

FIGURE:
Graphs help to analyze monitoring data

Conclusion

Only an all-encompassing security strategy can offer companies sufficient protection in the context of risk management. Network monitoring serves as a supplementary, strategically important module in IT security, which should go above and beyond the use of firewalls and virus scanners. In order to ensure the entire company network is protected as strongly as possible against malware attacks or failure, all IT areas must be monitored. Recognition of trends and developments is a significant factor in exposing looming threats. Network monitoring software provides the early warning system required, making it a useful extension to the security strategy that helps to establish the desired security and control for the company.

ABOUT PAESSLER AG

Paessler AG leads the industry in providing the most powerful, affordable and easy-to-use network monitoring and testing solutions. The company's suite of just-right software products deliver peace of mind, confidence and convenience for businesses of all sizes – from Small Office/Home Office (SOHO) to large enterprises, including more than 70% of the Fortune 100 companies. Based in Nuremberg, Germany, Paessler's global reach includes more than 150,000 active installations of its products. Founded in 1997, Paessler AG remains a privately held company and is recognized as both a member of the Cisco Solution Partner Program and a VMware Technology Alliance Partner.

Freeware and Free Trial versions of all products can be downloaded from www.paessler.com/prtg/download.

Paessler AG · www.paessler.com · info@paessler.com