SwiftWing
SIRIUS

Data Center Perspective

Data centers managers are always responsible when there are data intrusions, corruptions, leaks, and all sorts of services disruption. For those reasons, they need to have a full view of the network architecture and its traffic that passes in and out. Even with up to date security system such as IDS, IPS deployed, there could be a potential attacks that get pass into the core network.

When an attack happen, the conventional method will be digging out the access log files that are considered scattering, this is time-consuming even at the data collection stage. Some of the attack does not even leave any traces behind and it is difficult for investigation at post event.

The role of capture system comes in when recorded data can act as an evidence or source of investigation against illegal intruders. Because of the passive nature of capture system, it can be installed at the DMZ so that everything is being recorded:

i. "Build to capture and store anything within the network"

Cyber-attack post event analysis requires detailed information on every packets that traverse through the network. The technology of capturing data at high traffic inline rate (up to 40Gbps) and store to disk are highly sought after in order to have a versatile back up when catastrophic data event happens.

ii. "Fastest way of observing network traffic, statistically"

Real-time statistics reveals network traffic patterns and bandwidth usage. The live monitoring provides in-depth (up to OSI transport layer) counters as well as packet decoder for better visualization of network condition. All packets can be recovered because everything is captured and stored to disk.

iii. "Sync capture to centralized time source at finest resolution"

The synced time source to the capture system guarantees the captured data timestamp are accurate and reliable. The capture engine is able to resolute timestamp up to a nanosecond precision, allowing packets to have precise sequencing. In the case of network traffic burst, it is useful to recover the exact event even in one second (there are 1,000,000,000 nanosecond units in 1 second).

iv. "Multi-level privilege user access"

Collaboration team can have separable roles and so the capture system. Management group can have access to capture controls; Monitoring group will only have access to view live statistics; Analyst group can only view captured files to download and so on. Working with SIRIUS capture system optimizes the resources and more focus can be allocated for information searching.

v. "Comprehensive captures management, archiving finest details"

Compatible with network management system, in the event of illegal traffic detected at Firewall, the SNMP(v2) trap is able to trigger SIRIUS into capture file locking mode. This process further enhances automated file archiving even if the storage space on disk has reached its very limit.

Contact Information:

ComWorth Co., Ltd.
2-35-7, Nishi Magome
Ohta-ku, Tokyo,
143-0026, Japan
Tel: +81 3 3777 0888
Fax: +81 3 3772 8497
info2@comworth.co.jp

ComWorth Solutions Pte. Ltd
81 Ubi Avenue 4,
#06-02 UB.One,
Singapore 408830
Tel 1: +65 6748 2260
Tel 2: +65 6909 5198
info@comworth.com.sg

ComWorth Europe GmbH
Gutenbergstrasse 5
D-65830 Kriftel
Germany
Tel +49 (0) 6192 922 4227
Fax +49 (0) 6192 922 4228
contact@comworth.eu
www.swiftwing.net

WEEE Nr.: DE41316630
D-U-N-S No. 313277272

MADE IN JAPAN 日本製