saisei

Next Generation NETWORK SECURITY

Security for computer networks and systems is a very broad and multi-faceted subject, addressed by a wide variety of tools and applications. Saisei's FlowCommand has powerful real-time flow tracking, analysis and correlation capabilities. These can enhance an existing total security solution with unique capabilities, and replace some existing network security functions such as firewalls.

FlowCommand uses unique flow correlation algorithms to detect a variety of network-based threats and attacks. Once a threat is detected, there are several ways it can be mitigated. In addition, the powerful alarm and reporting mechanisms can be used to notify network operations personnel or to take action elsewhere in the network or data center.

Saisei FlowCommand can be deployed in conjunction with specialised security systems in order to leverage Saisei's advanced flow inspection and correlation algorithms with its next generation traffic management features to provide unprecendeted attack idenficiation and mitigation features.

Attack Mitigation and Reporting

When an attack is detected, there are several ways to react. Often, it is desirable to block the specific attacking flow. Saisei FlowCommand can extend that to block all traffic from the source of the attack. The standards for the Internet define "BGP Flowspec" which allows a network device, such as FlowCommand, to direct the next-level service provider to suppress traffic matching a specified pattern, preventing such traffic from even reaching the network under attack.

Sometimes blocking the traffic is not desirable. Saisei FlowCommand can divert all attack traffic to a dedicated analysis system, or limit its rate so there are no adverse effects on the rest of the network.

Saisei's powerful and versatile alarm mechanism can be triggered by the detection of an attack and configured to take any required action. For example, it can notify a security alert system, or run a script that triggers protection mechanisms elsewhere in the network or data center.

Saisei as Firewall

The network firewall is the oldest form of network protection. In its simplest form, it allows traffic to be accepted or rejected based on the IP address of its source or destination, or the protocol in use, as identified by the TCP or UDP port number. Such firewalls have been around since the earliest days of the Internet.

So-called "next generation" firewalls allow traffic to be managed based on more complex analysis of the traffic. Applications can be identified by deep packet inspection (DPI), and by correlating activity on multiple flows. Once the application is known, it can be used as an input to the firewall's decisions. Saisei FlowCommand supports this function, and furthermore can use information about the geolocation of the traffic (e.g. country) and BGP routing information. It can take into account characteristics of individual flows. For example, a long flow may be a data exfiltration attack and requires different analysis than a short flow containing little data

.

Probing Attacks

All networks are constantly being probed for vulnerable hosts. Attackers try all combinations of IP address and port number to look for attack victims. Not only is this a security risk, it also needlessly consumes network bandwidth.

FlowCommand understands the random nature of probing attacks, and uses that together with correlation of multiple flows to identify attacking hosts. These can then be blocked, or diverted to specialized security analysis systems.

Protocol-Based Attacks

The protocols used in the Internet were designed a long time ago, before the possibility of malicious traffic was ever considered. As a result they have many security vulnerabilities which have been exploited over the years. Generally these have been mitigated by changes to code in hosts and routers, but there remains the possibility of new exploits and of unpatched systems which remain vulnerable.

FlowCommand detects many kinds of protocol misbehavior. It may indicate an attack or a new exploit, or simply a bug or misconfiguration elsewhere in the network, but it is not normal behavior. It can respond to this by blocking the errant flow, and by blocking the originating system.

Address Spoofing

It is common for hosts to generate traffic with an address which is not their own – called "address spoofing". Service providers could detect and block this, but mostly they don't. It can cause particular problems when external hosts use addresses which correspond to addresses within the protected network. FlowCommand can detect this and block such traffic.

Distributed Denial of Service (DDoS) Attacks

DDoS attacks focus a vast excessive amount of traffic on a single host. Usually, the intent is to make it inaccessible, hence the name "Denial of Service". Some very large scale attacks have even made non-technical news, but smaller scale attacks occur constantly, often without any obvious motivation. Not only do they disrupt the attacked host, they also cause network congestion for other users. Typically they are generated using botnets, containing up to millions of distinct hosts and controlled from a central point. The traffic looks legitimate and it is almost impossible to distinguish from an unusually heavy load.

FlowCommand can detect unusually high levels of activity, using its "machine learning" feature which constantly compares current activity (bandwidth, flow setup rate, etc) with historical levels. It can then block the attacking traffic, including the use of BGP Flowspec to block it remotely.

Internal Attacks and Exploits

A service provider with thousands of customers can never be sure that attacks and exploits are not occurring within their own network. Apart from the possible damage in the Internet in general, such attacks can disrupt and overload the internal network. FlowCommand can detect many such exploits, generating an alarm to netops personnel or even, if desired, blocking the internal user.

Host and URL Reputation

Extensive databases have been built describing hosts which are malicious or responsible for inappropriate content. Some of these are freely available, while others require a subscription.

STM can load these databases and use them to direct the handling of flows. Hosts are identified directly from the IP addresses in flows. URLs are identified by examining the HTTP or HTTPS payload.

The appropriate action depends on the reason for the listing. Malicious traffic will most probably be dropped. Other traffic, such as pornography, may be passed or dropped depending on the user's profile, or may be subject to a rate limit.

saisei

Saisei is a Sunnyvale, California-based software company that is revolutionizing network analysis and control for the challenges that mobility, cloud, SDN, NFV, and the Internet of Things are bringing to networks today. Its scalable, real-time Network Performance Enforcement software solutions provide the speed and smarts needed to instantly analyze and enforce policy on the millions of applications, users, and devices populating networks today. Enterprises and service providers can now use their full network bandwidth knowing that unexpected traffic surges are automatically accommodated and all user traffic will get through even the busiest of network links with no dropped sessions, resulting in dramatic savings, accelerated revenue growth and a great user experience.

Learn more at

www.saisei.com

Connect with Saisei

info@saisei.com

+1 669.224.4392

USA
710 Lakeway Drive, Suite 290
Sunnyvale, CA 94085 USA

ASIA
10 Anson Road #26-04
International Plaza Singapore 079903

AUSTRALIA
Level 6, 10 Queens Road
Melbourne VIC 3004 Australia