Network Performance Enforcement Solutions

Introduction

Despite the increased capacity available on WAN links, service providers and enterprises often find bandwidth in short supply. This occurs even though most links average only 30%-40% utilization, and at best 50%-70% when specialized equipment is used. Today's best practice is to reserve significant capacity, often half of the total link capacity, to ensure a constant data flow during traffic surges and bandwidth-hogging application sessions, such as peer-to-peer downloads.

This unfortunate situation is due to the chaotic and random nature of TCP/IP best effort delivery. In a best-effort network all users obtain unspecified variable bit rate and delivery time, depending on the current traffic load. When used with quality of service (QoS) and other priority controls, best effort has worked moderately well for many years. The physical size and extent of the Internet and new traffic patterns, however, have made it less and less effective.

Saisei uses a patented technology that empowers WAN link utilization at 95% or better, without loss of connections, delay in traffic flow, queuing, or buffering. Under policy control, every user gets a fair and equitable share of the bandwidth, with high quality of experience (QoE). Saisei's products FlowVision™, and FlowCommand™ run virtual machines (VM), dedicated server or on our branded devices.

Challenge

Carriers and cloud service providers must ensure that applications hosted at their facilities deliver high QoE without service interruptions. Enterprise IT organizations must guarantee reserved bandwidth for communications with business-critical, cloud-based infrastructure components. At the same time, misbehaving applications and users must be prevented from degrading overall network performance.

Multiple devices are used today to optimize bandwidth, including WAN optimizers, packet shapers, application delivery controllers (ADC), load balancers, advanced routers, and next-generation firewalls. There are also a number of application performance monitoring (APM) and network performance monitoring (NPM) tools that are used to maintain networks. These devices are expensive to purchase, configure, and maintain and in some cases their functions may interfere with each other.

Even with existing technologies and optimization devices, service providers and enterprises must pay for overcapacity in order to handle surges and high-bandwidth applications and users. This is still only a partial solution; companies are rife with angry users who are disappointed with the service they receive.

Solution

Saisei is an early leader in a new field of network optimization called Network Performance Enforcement (NPE). NPE represents a class of solutions that combine real-time, in-line visibility, control, and security of application flows in a unified, scalable architecture designed for the modern, federated world of mobile, cloud, and Internet of things (IoT) data.

Saisei's FlowCommand offers a means of unifying network traffic and security monitoring, visibility, and control. Using FlowCommand, service providers and enterprises can achieve high utilization on their WAN links without delaying traffic flow or introducing queuing or buffering. FlowCommand is engineered to ensure that no user session will ever crash or time out. FlowCommand implements policy-based rate protection, not limitation, enforcing bandwidth based on a number of criteria:

- **Per-user.** Users can all receive the same rate with net neutrality or can be assigned preferred rates. Active Directory Integration required.
- **Per-host / subnet.** All traffic from a host can be aggregated and controlled.
- **Per-application / application group.** Different applications have different rate requirements. A library of more than 10,000 applications is maintained by FlowCommand. Deep packet inspection (DPI) is used to identify applications with new apps automatically added to the list as they are recognized. Critical applications can be guaranteed bandwidth while non-critical or undesirable applications can be limited, diverted, or blocked.
- **By geography.** Using geolocation techniques and custom fields, FlowCommand attempts to locate the destination for traffic flows.
- **Per MPLS label.** The overall bandwidth of MPLS tunnels is controlled as well as the traffic within the tunnels.
- **For custom groups,** using any combination of characteristics described above. For example, a custom group could identify all countries with a company's offices. That group could be used to limit database access from only those countries to normal business hours.

The result is predictable and equitable performance for all users. Figure 1 shows how FlowCommand's net neutrality equalization changes the chaotic real-time rates (upper graph) to an assignment in which all users receive the same rate (lower graph).

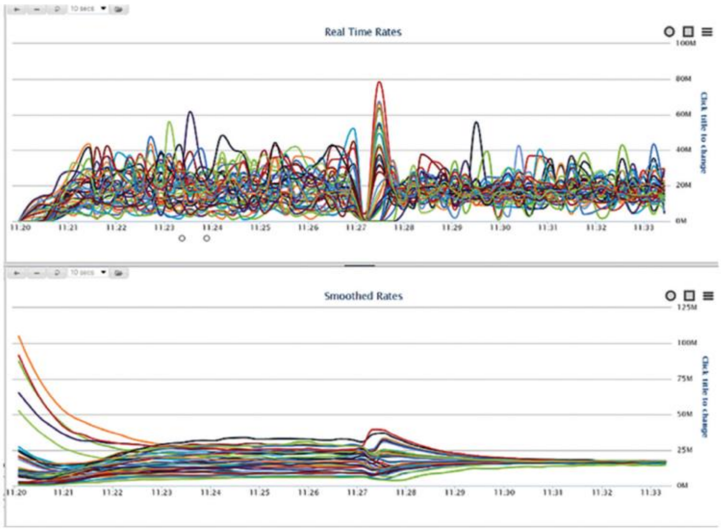

FIGURE 1 - SAISEI FLOWCOMMAND'S NET NEUTRALITY

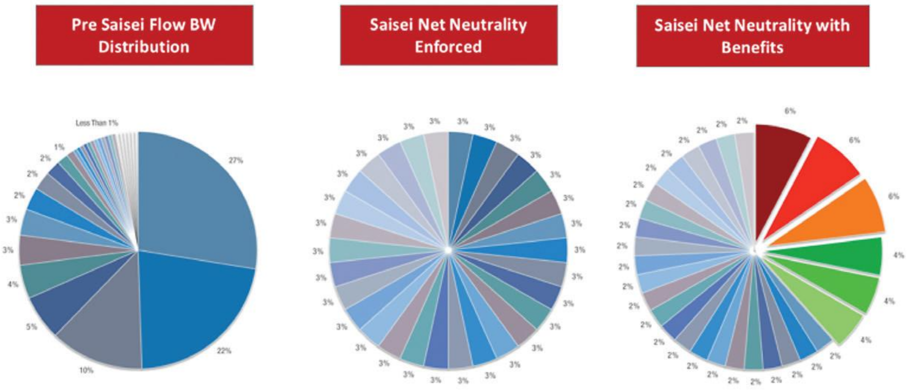

Figure 2 illustrates how FlowCommand allows specific users to receive differentiated service. Each slice represents the percentage of total bandwidth for each user.

FIGURE 2 - NET NEUTRALITY WITH DIFFERENTIATED SERVICE

How FlowCommand Works

FlowCommand is placed in-line with traffic flow from a WAN link, so that all traffic for that link is monitored and/or controlled. It may be used on one or both ends of a WAN link.

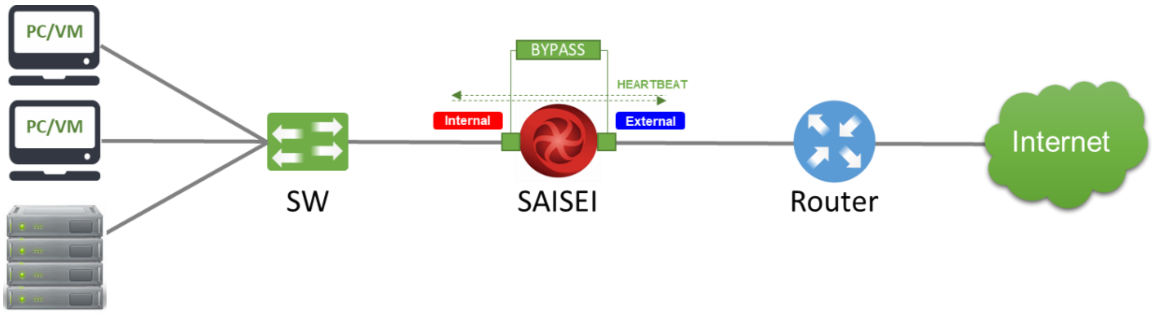

FIGURE 3 - TYPICAL FLOWCOMMAND™ DEPLOYMENT SCENARIO

Saisei has verified each instance of FlowCommand can control 5 million flows at up to 10 Gbps. Traffic is analyzed 20 times per second using 40 fine-grained metrics. An independent process and sophisticated GUI is used to visualize traffic and to manage policies. FlowCommand implements flow control based on four patents: slight delays are introduced into flows by inserting microsecond resolution pauses and/or by dropping selected packets. FlowCommand is designed to have a minimal impact on traffic delay, typically introducing only 5-6 microseconds of delay, which is a significant improvement of the delay associated with the average best next-gen firewalls.

Policy management may be performed with Saisei's own GUI, or may be controlled through its RESTful API. The API allows FlowCommand and its subsets to be integrated into a SDN network or with other NFV components.

Real-Time Monitoring

FlowVision provides a high resolution, real-time view of network traffic using 40 metrics – performing many of the functions of classical APM/NPMs. Network administrators view usage by user, application, host, or geolocation. They can display rates, throughput, protocols, and flow control information. Flow data can be exported via the industry-standard IPFIX protocol for integration with other tools. FlowVision is particularly valuable for real-time troubleshooting since it allows rapid drill down to user, application, and server.

Security

FlowCommand is used to augment existing security measures at the edge of a network, principally through real-time mitigation of attacks. For example, it can be used to effectively defend against botnet and DDoS attacks through policies that limit the number of active sessions for a given protocol or port. Policies that identify foreign sites and hours of permitted access allow FlowCommand to control when enterprise applications may be used, limiting data exfiltration. Flows can be selectively redirected to other security processors, such as intrusion detection or prevention systems (IDS/IPS), as necessary.

Key Features

- **Powerful Real-Time Visibility, Monitoring & Analytics.** Deeper visibility, real-time applications distress monitoring & alerts. May be used for troubleshooting and tuning.
- **Increased bandwidth utilization.** Increased bandwidth without delaying traffic or causing loss of connections.
- **Bandwidth rate protection.** Policy-based control of rate on a per-user, per-application, per-host, per-location basis.
- **Advanced policy management.** GUI- or API- based policy rules dictate which users and applications receive bandwidth.
- **Fair Usage.** Allow each user (host/VLAN) to receive fair share (or controller unfair share per SLA) of the network. Host Equalization.
- **Augmented security.** Real-time monitoring allows FlowCommand to fend off attacks and to prevent unauthorized access.
- **Threat & Attack Detection, Report & Control**. Monitors traffic anomalies corresponding to various type of attacks (DDoS, TCP SYNC, Address Spoofing, Exploits) and triggers alarms.
- **Inexpensive.** Less than the maintenance cost of a comparable WAN optimization system and packet shapers.

Other Features

VISIBILITY

- Dynamic Application Detection based on signatures, URLs and powerful heuristics allowing flow correlation
- Custom Application / Custom Group Application
- Flow-Rate Monitoring
- TCP Flow Health Monitoring
- Application Health Scores
- Network Performance Metrics
- Historical Visibility till 2 years
- User configurable filters, and unlimited combinations, for deeper analysis
- Download Report
- Automated reports
- Customizable Dashboard reports

CONTROL

- Multi policies
- Min & max bandwidth policies
- Behavior-Based Flow Control
- Time based controls
- Manage Bandwidth by customer & plans / quotas
- QoS / QoE / Mark DSCP
- Unlimited priority levels
- Control both inbound and outbound directed traffic independently

ALERTS, ALARMS & ACTIONS

- Alerts for conditions
- Alarms & Automated Actions like run scripts
- Alarms by SNMP (Traps), syslog & email

NETWORK

- Port/Interface
- Policy-Based Routing
- Inline/Span/Tap Ports
- VLAN/VxLAN
- MPLS tunnels
- GRE
- IPv4/IPv6
- Bridge bypass

MANAGEMENT

- SSHv2
- REST API for easy integration
- SNMP
- Python
- Comprehensive GUI / CLI
- Radius Signaling
- Netflow export
- Updates remotely

Saisei Hardware Specifications

	Saisei STM-2G
Visibility and Policy Control	
Shaping Throughput Full-Duplex	Up to 2Gbps
Concurrent Flows	2,000,000
Packets Per Second	1,000,000/s
Recommended Users	30,000
Networking	
Ethernet Interface	4 x 1 Gigabit Copper
Ethernet Bypass Bridge Pairs	2
Management Interface	2 x 1 Gigabit Ethernet Copper
Serial Console	1 x RJ45 RS232 console
USB	2 x USB 2.0
Network Interface Card (NIC) Module slot	1
Available NIC	4 x 1Gigabilt (2 bypass bridge pair) 2 x 10Gigabilt (1 bypass bridge pair)
Physical Characteristics	
Platform	8 cores / 16 GB RAM / 500 GB SSD
Form Factor	Standard 1UR by 19" rack mount
Unit Dimensions (WxHxD)	431 x 44 x 305 mm
Unit Weight	4 kg
Power Supply Unit	50W ATX Power Supply AC 100~240 V @50~60 Hz
Operating temperature	0°C to 40°C
Approvals and Compliance	CE Class A, FCC Class A, UL, RoHS
Hardware warranty	12 months

ABOUT 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 busiest of networks links with no dropped sessions, resulting in dramatic savings, accelerated revenue growth and great user experience.

Learn more at

www.saisei.com