FirstWave

Network Performance Enforcement Solutions

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% utilisation, and at best 50%-70% when specialised 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 an 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.

FirstWave uses a technology that empowers WAN link utilisation 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). FirstWave's Secure Traffic Manager (STM) runs virtual machines (VM), dedicated servers, or on our branded devices.

The Challenge

Carriers and cloud service providers must ensure that applications hosted at their facilities deliver high QoE without service interruptions. Enterprise IT organisations 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 optimise bandwidth, including WAN optimisers, packet shapers, application delivery controllers (ADCs), 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 optimisation 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.

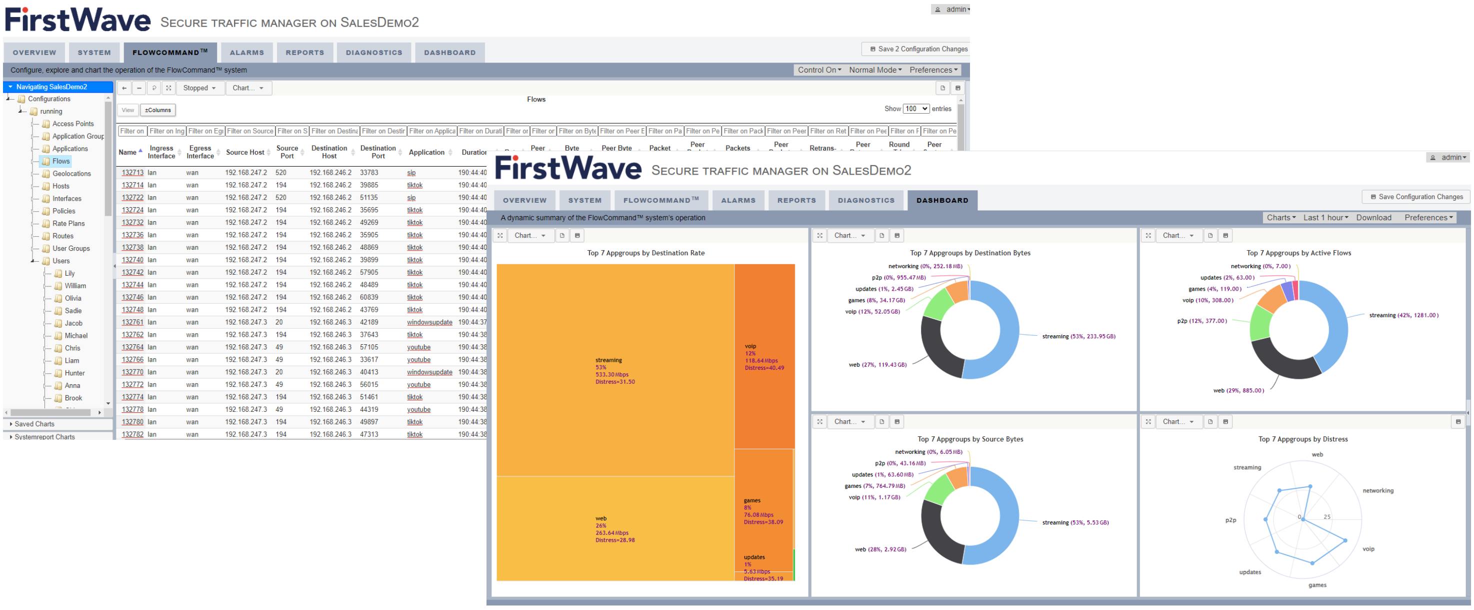
The Solution

FirstWave is an early leader in a new field of network optimisation 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.

STM offers a means of unifying network traffic and security monitoring, visibility, and control. Using STM, service providers and enterprises can achieve high utilisation on their WAN links without delaying traffic flow or introducing queuing or buffering. STM is engineered to ensure that no user session will ever crash or time out. It 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 STM. Deep Packet Inspection (DPI) is used to identify applications with new apps automatically added to the list as they are recognised. 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, STM 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.



Configure, explore and chart the operation of the FlowCommand™ system

Flows

Name	Ingress Interface	Egress Interface	Source Host	Source Port	Destination Host	Destination Port	Application	Duration
132713	lan	wan	192.168.247.2	520	192.168.246.2	33783	sip	190:44:40
132714	lan	wan	192.168.247.2	194	192.168.246.2	39885	tiktok	190:44:40
132722	lan	wan	192.168.247.2	520	192.168.246.2	51135	sip	190:44:40
132724	lan	wan	192.168.247.2	194	192.168.246.2	35695	tiktok	190:44:40
132732	lan	wan	192.168.247.2	194	192.168.246.2	49269	tiktok	190:44:40
132736	lan	wan	192.168.247.2	194	192.168.246.2	35905	tiktok	190:44:40
132738	lan	wan	192.168.247.2	194	192.168.246.2	48869	tiktok	190:44:40
132740	lan	wan	192.168.247.2	194	192.168.246.2	39899	tiktok	190:44:40
132742	lan	wan	192.168.247.2	194	192.168.246.2	57905	tiktok	190:44:40
132744	lan	wan	192.168.247.2	194	192.168.246.2	48489	tiktok	190:44:40
132746	lan	wan	192.168.247.2	194	192.168.246.2	60839	tiktok	190:44:40
132748	lan	wan	192.168.247.2	194	192.168.246.2	43769	tiktok	190:44:40
132761	lan	wan	192.168.247.3	20	192.168.246.3	42189	windowsupdate	190:44:37
132762	lan	wan	192.168.247.3	194	192.168.246.3	37643	tiktok	190:44:38
132764	lan	wan	192.168.247.3	49	192.168.246.3	57105	youtube	190:44:38
132766	lan	wan	192.168.247.3	49	192.168.246.3	33617	youtube	190:44:38
132770	lan	wan	192.168.247.3	20	192.168.246.3	40413	windowsupdate	190:44:38
132772	lan	wan	192.168.247.3	49	192.168.246.3	56015	youtube	190:44:38
132774	lan	wan	192.168.247.3	194	192.168.246.3	51461	tiktok	190:44:38
132778	lan	wan	192.168.247.3	49	192.168.246.3	44319	youtube	190:44:38
132780	lan	wan	192.168.247.3	194	192.168.246.3	49897	tiktok	190:44:38
132782	lan	wan	192.168.247.3	194	192.168.246.3	47313	tiktok	190:44:38

A dynamic summary of the FlowCommand™ system's operation

How Secure Traffic Manager Works

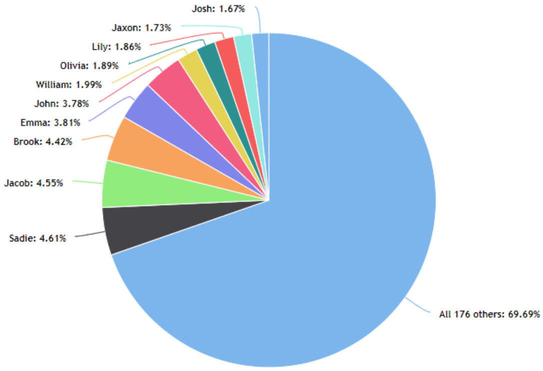
STM is placed in-line with traffic flow from a WAN link, so that all traffic for that link is monitored and/or controlled. It may be used on one or both ends of a WAN link.

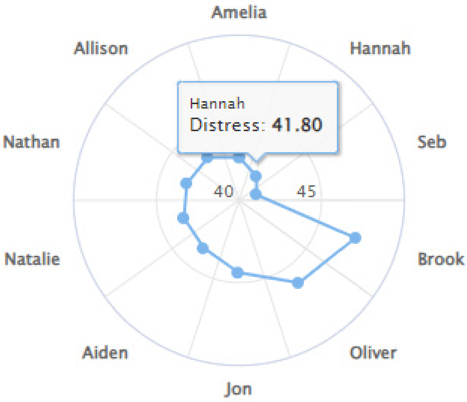
FirstWave has verified that each instance of STM can control five million flows at up to 10 Gbps. Traffic is analysed 20 times per second using 40 fine-grained metrics. An independent process and sophisticated GUI is used to visualise traffic and to manage policies.

STM implements flow control based on four patents: slight delays are introduced into flows by inserting microsecond resolution pauses and/or by dropping selected packets.

STM is designed to have a minimal impact on traffic delay, typically introducing only 5-6 microseconds of delay, a significant improvement to the delay associated with the average best next-gen firewalls.

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



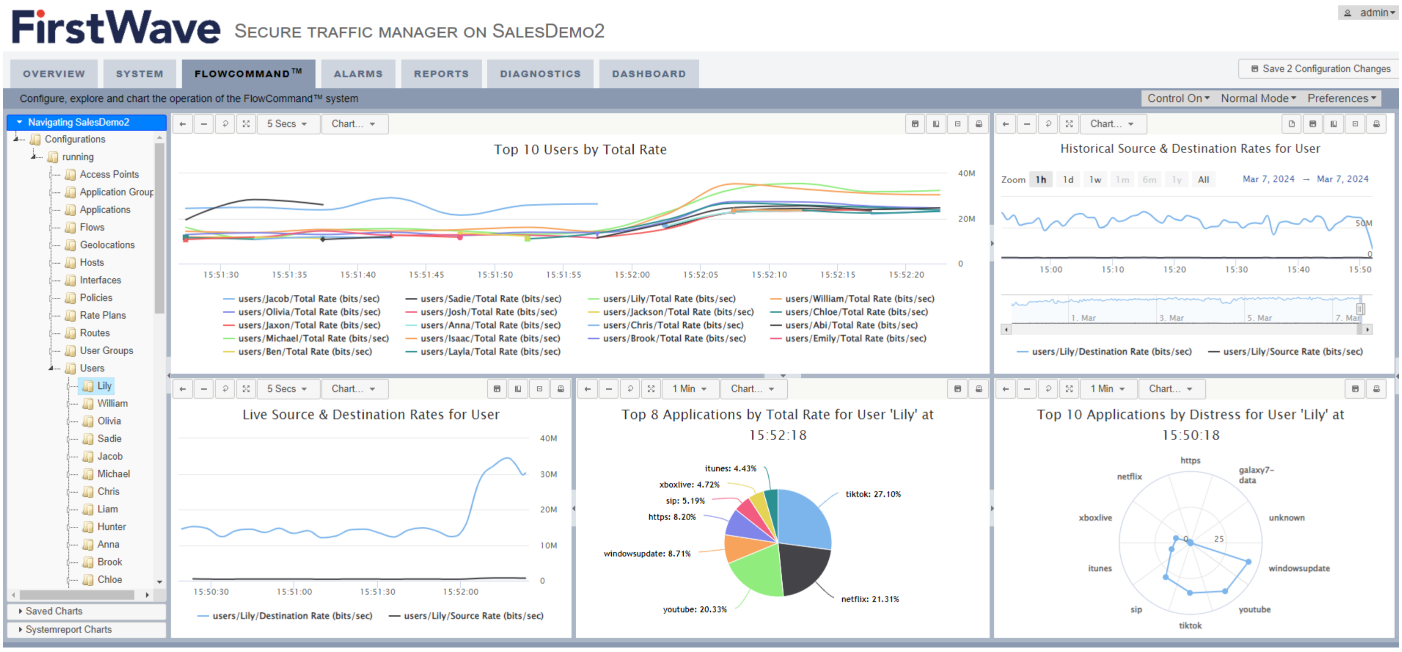


Real-Time Monitoring

STM 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. This feature is particularly valuable for real-time troubleshooting as it allows rapid drill down to user, application, and server.

Security

STM 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 STM 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.


FirstWave SECURE TRAFFIC MANAGER ON SALESDEMO2

Configure, explore and chart the operation of the FlowCommand™ system

admin
OVERVIEW
SYSTEM
FLOWCOMMAND™
ALARMS
REPORTS
DIAGNOSTICS
DASHBOARD
Save 2 Configuration Changes
Control On
Normal Mode
Preferences
Navigating SalesDemo2
Configurations
running
Access Points
Application Group
Applications
Flows
Geolocations
Hosts
Interfaces
Policies
Rate Plans
Routes
User Groups
Users
Lily
William
Olivia
Sadie
Jacob
Michael
Chris
Liam
Hunter
Anna
Brook
Chloe
Saved Charts
Systemreport Charts
5 Secs
Chart...
Top 10 Users by Total Rate
40M
20M
0
15:51:30
15:51:35
15:51:40
15:51:45
15:51:50
15:51:55
15:52:00
15:52:05
15:52:10
15:52:15
15:52:20
users/Jacob/Total Rate (bits/sec)
users/Olivia/Total Rate (bits/sec)
users/Jaxon/Total Rate (bits/sec)
users/Michael/Total Rate (bits/sec)
users/Ben/Total Rate (bits/sec)
users/Sadie/Total Rate (bits/sec)
users/Josh/Total Rate (bits/sec)
users/Anna/Total Rate (bits/sec)
users/Isaac/Total Rate (bits/sec)
users/Layla/Total Rate (bits/sec)
users/Lily/Total Rate (bits/sec)
users/Jackson/Total Rate (bits/sec)
users/Chris/Total Rate (bits/sec)
users/Brook/Total Rate (bits/sec)
users/William/Total Rate (bits/sec)
users/Chloe/Total Rate (bits/sec)
users/Abi/Total Rate (bits/sec)
users/Emily/Total Rate (bits/sec)
Chart...
Historical Source & Destination Rates for User
Zoom 1h 1d 1w 1m 6m 1y All
Mar 7, 2024 → Mar 7, 2024
50M
0
15:00
15:10
15:20
15:30
15:40
15:50
1. Mar
3. Mar
5. Mar
7. Mar
users/Lily/Destination Rate (bits/sec)
users/Lily/Source Rate (bits/sec)
5 Secs
Chart...
Live Source & Destination Rates for User
40M
30M
20M
10M
0
15:50:30
15:51:00
15:51:30
15:52:00
users/Lily/Destination Rate (bits/sec)
users/Lily/Source Rate (bits/sec)
1 Min
Chart...
Top 8 Applications by Total Rate for User 'Lily' at 15:52:18
itunes: 4.43%
xboxlive: 4.72%
sip: 5.19%
https: 8.20%
windowsupdate: 8.71%
youtube: 20.33%
tiktok: 27.10%
netflix: 21.31%
1 Min
Chart...
Top 10 Applications by Distress for User 'Lily' at 15:50:18
https
galaxy7-data
unknown
windowsupdate
youtube
tiktok
sip
itunes
xboxlive
netflix
0
25

Key Features

- **Powerful real-time visibility, monitoring, and analytics.** Deeper visibility, real-time application distress monitoring, and alerts may be used for troubleshooting and tuning.
- **Increased bandwidth utilisation.** Increased bandwidth without delaying traffic or causing loss of connections.
- **Bandwidth rate protection.** Policy-based rate control 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.** Allows each user (host/VLAN) to receive fair share (or controller unfair share per SLA) of the network. Host equalisation.
- **Augmented security.** Real-time monitoring allows STM to fend off attacks and to prevent unauthorised access.
- **Threat and attack detection, report, and control.** Monitors traffic anomalies corresponding to various types of attacks (DDoS, TCP SYNC, address spoofing, exploits) and triggers alarms.
- **Inexpensive.** Less than the maintenance cost of a comparable WAN optimisation 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
- Operating system visibility
- Historical visibility of up to two years
- User configurable filters, and unlimited combinations, for deeper analysis
- Download report
- Automated reports
- Customisable dashboard reports

Control

- Multi policies
- Min. and max. bandwidth policies
- Behaviour-based flow control
- Time based controls
- Manage bandwidth by customers and plans/quotas
- QoS/QoE/Mark DSCP
- Unlimited different priority levels
- Control both inbound and outbound directed traffic independently

Alerts, Alarms, and Actions

- Alerts for conditions
- Alarms and automated actions like run scripts
- Alarms by SNMP (traps), syslog, and 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 signalling
- Netflow export
- Updates remotely

STM for FirstWave Hardware Specifications

	STM-EO	STM-2G	STM-10G	STM-HCPro	STM-100G
Visibility and Policy Control					
Shaping Throughput Full-Duplex	Up to 250 Mbps	Up to 2 Gbps	Up to 10 Gbps	Up to 20 Gbps	Up to 100 Gbps
Concurrent Flows	180,000	2,000,000	9,000,000	18,000,000	60,000,000
Packets Per Second	75,000/s	1,000,000/s	4,000,000/s	8,000,000/s	25,000,000/s
Networking					
Ethernet Interface	3 x 1GE RJ45	4 x 1GE RJ45	2 x 10G FO 4 x RJ45	-	-
Ethernet Bypass Bridge Pairs	1	Up to 4 x 1GE Up to 1 x 10GE	Up to 4 x 1GE Up to 2 x 10GE	Up to 16 x 1GE Up to 8 x 10GE	Up to 32 x 1GE Up to 16 x 10GE Up to 4 x 40/100GE
Management Interface	1 x 1GE RJ45	2 x 1GE RJ45	2 x 6GE RJ45	1 x 1GE RJ45	SS
Serial Console	1 x RJ45	1 x RJ45	1 x RJ45	1 x RJ45	1 x RJ45
USB	2 x USB 3.0	2 x USB 2.0	2 x USB 3.0	2 x USB 3.0	2 x USB 2.0 1 x USB 3.0
Network Interface Card (NIC) Module Slot	-	1	1	8	8
Physical Characteristics					
Form Factor	Tabletop	1U 19" Rackmount	1U 19" Rackmount	2U 19" Rackmount	2U 19" Rackmount
Unit Dimensions (WxDxH) (mm)	146 x 118 x 34	431 x 305 x 44	431 x 305 x 44	438 x 600 x 88	434 x 736 x 87
Unit Weight	0.6 kg	4 kg	4 kg	24 kg	36 kg
Power Supply Unit	W Power Adapter AC 100~240V @50~60Hz, 3A	150W ATX Power Supply AC 100~240 V @50~60 Hz	150W ATX Power Supply AC 100~240 V @50~60 Hz	850W 1+1 ATX Redundant PSUs AC 100V~240V @47~63Hz	1100W 1+1 ATX Redundant PSUs AC 100V~240V @47~63Hz
Operating Temperature	0°C to 40°C	0°C to 40°C	0°C to 40°C	0°C to 40°C	0°C to 40°C
Approvals and Compliance	CE/FCC Class B, UL, RoHS	CE/FCC Class A, UL, RoHS	CE Class A, FCC Class A, UL, RoHS	CE/FCC, UL, RoHS	CE/FCC, UL, RoHS

Available NIC Module

STM-4X1GE	Network Extension Module - 4 ports 1GE RJ45 ethernet with 2 pairs bypass
STM-4X10GFB-SR	Network Extension Module - 4 ports 1G fibre short-range (multi-mode) with 2 pairs bypass
STM-2X10GE	Network Extension Module - 2 ports 10GE RJ45 ethernet with 1 pair bypass
STM-2X10GFB-SR	Network Extension Module - 2 ports 10G fibre short-range (multi-mode) with 1 pair bypass
STM-4X10GFB-SR	Network Extension Module - 4 ports 10G fibre short-range (multi-mode) with 2 pairs bypass

FirstWave
www.firstwave.com
connect@firstwave.com
+61 2 9409 7000

USA
1 Harbor Dr Suite 300
Sausalito, CA 94965

AUSTRALIA
Level 14, 132 Arthur Street
North Sydney NSW 2060

Learn more at firstwave.com/stm