SOLUTION BRIEF

Brocade Flow Optimizer

HIGHLIGHTS

- Provide real-time network visibility with policy based detection and management of large Layer 2 through Layer 4 traffic flows
- Improve overall customer experience with proactive traffic engineering and eliminate network congestion
- Avoid expensive network failures and service interruptions as a result of large Layer 2 through Layer 4 volumetric traffic attacks
- Gain real-time event logging and traffic statistics using a simple and user-friendly, Web-based Graphical User Interface (GUI)
- Easy integration with third-party cloud orchestration systems with the support of REST APIs

Delivering Real-Time, Intelligent, and Policy-Based Flow Management

Today's static and manually provisioned networks continue to demonstrate unpredictable network behavior, posing challenges for service provider and enterprise customers. As more workloads shift into the cloud and Big Data becomes a significant portion of the network traffic, network performance management and large network flow visibility become critical requirements. Security is another key challenge for customers. Vulnerabilities, such as large volumetric traffic attacks that can penetrate and flood a network, can result in very serious consequences, including service disruptions and loss of revenue. Customers need network intelligence to manage their network more easily and to be able to proactively take action when needed.

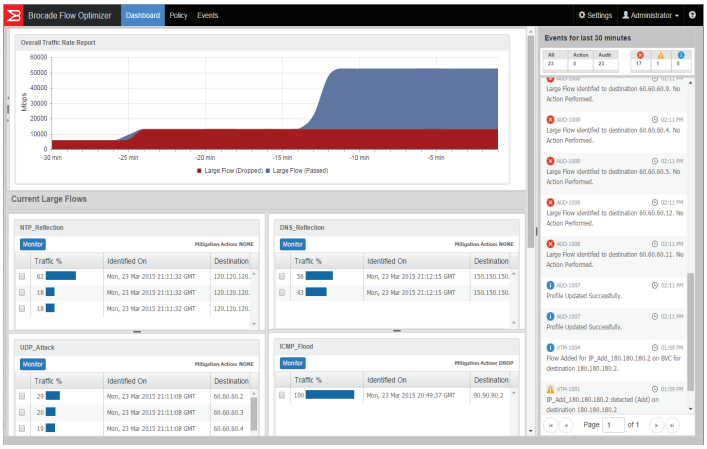

Figure 1. The Brocade Flow Optimizer GUI.

The Brocade Flow Optimizer Solution

The Brocade® Flow Optimizer is an open and agile policy-based Software-Defined Networking (SDN) solution that detects and manages large Layer 2 through Layer 4 traffic flows in service provider and enterprise networks. Customers can optimize their network infrastructure, increase network efficiency, and improve network resource utilization and capacity planning using this solution. As shown in Figure 2, the Brocade Flow Optimizer enables proactive traffic visibility and traffic engineering of the network, allowing customers to take specific actions based on established policies and in turn, eliminate network congestion and mitigate network attacks resulting from large volumetric traffic flows.

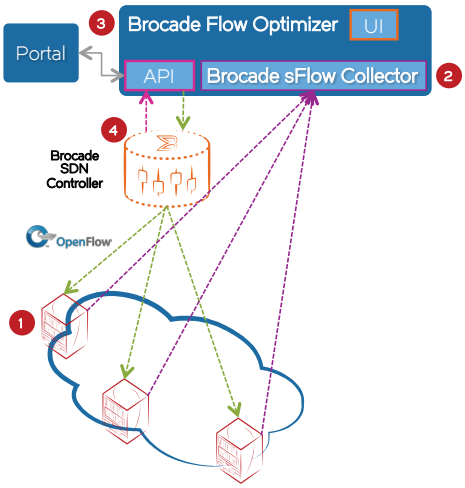

Figure 2. Brocade Flow Optimizer—An SDN-Based Application.

How Does It Work?

1. Brocade network devices, such as Brocade MLXe® Routers and Brocade ICX® Switches, send sFlows samples to the server where the Brocade Flow Optimizer application resides.
2. The sFlows samples are received by the built-in sFlow collector.
3. The Brocade Flow Optimizer analyzes the sFlows samples to detect traffic flows. Based on the policies that have been set and takes the appropriate actions defined in the respective policies. The actions include:
   - Discard
   - Rate limit
   - Remark
   - Redirect
4. The OpenDaylight-based Brocade SDN Controller programs OpenFlow version 1.3 rules in the Brocade network devices.

The Brocade Flow Optimizer enables customers to address numerous use cases and can be deployed seamlessly in a variety of networking scenarios.

Network Volumetric Attack Mitigation

Today security remains one of the top concerns in networking. Vulnerabilities and breaches can occur at any point in the network. One of the most common forms of network attack is Distributed Denial of Service (DDoS), which is a type of volumetric traffic flow attack.

Traditional DDoS mitigation solutions rely on specialized network appliances, which have limited capacity. As the amount of DDoS traffic increases, the number of such specialized appliances and recurring licensing fees also increases, making these traditional solutions not economically attractive or viable in the long term.

As shown in Figure 3, customers using the Brocade Flow Optimizer can enable policies to mitigate certain DDoS types of attacks. Based on built-in or customer-defined policies, customers can identify malicious traffic flows and take the appropriate actions at the edge of the network, whether it's dropping, rate limiting, remarking, or redirecting the malicious traffic flows. While the

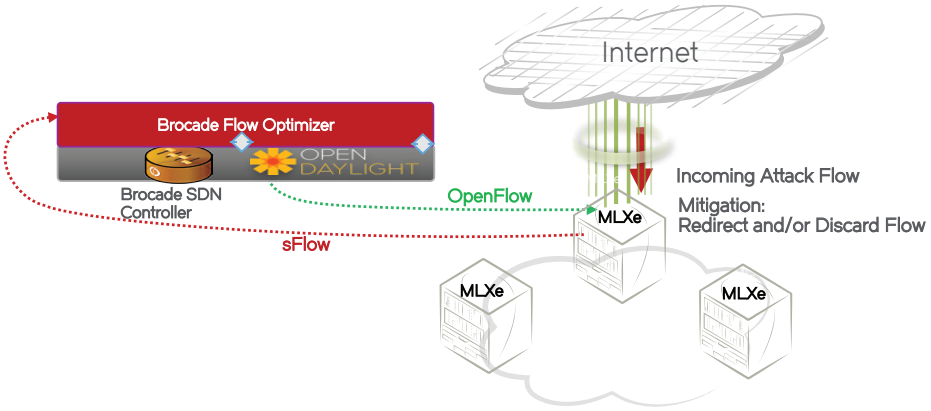

Figure 3. Network Volumetric Attack Mitigation with the Brocade Flow Optimizer.

built-in policies only cover a small fraction of potential DDoS security types, they provide for a significant reduction in the total amount of potential DDoS traffic left to be mitigated by other devices, which leads to an overall reduction in DDoS mitigation costs. The Brocade Flow Optimizer provides an integrated, higher-performing, more scalable, and cost-competitive solution. Customers can significantly simplify their network operation as well as reduce operational cost.

Application Traffic Control

As shown in Figure 4, customers can use the Brocade Flow Optimizer to define specific policies, and in turn control specific application traffic. The policy describes the profile of the application traffic, such as the source IP address and UDP/TCP port address, and the minimum amount of traffic required to trigger the policy and the action to take when the policy is triggered. Actions include rate limit (meter), drop, QoS remark, and redirect. Customers can use this capability to limit the usage of certain applications (such as NetFlix) by denying access (drop), limiting amount of use (rate limit), or lowering or raising the priority (remark) for that specific application in lieu of other higher-priority traffic.

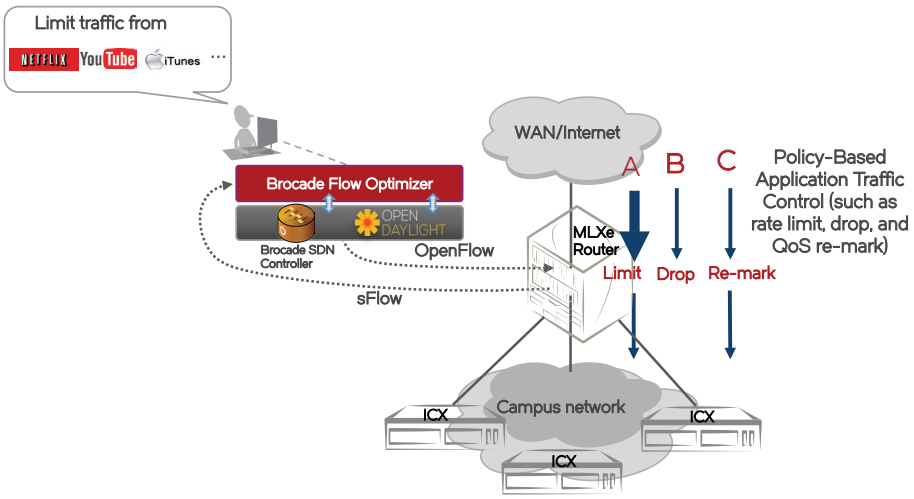

Figure 4. Brocade Flow Optimizer-Application Traffic Control.

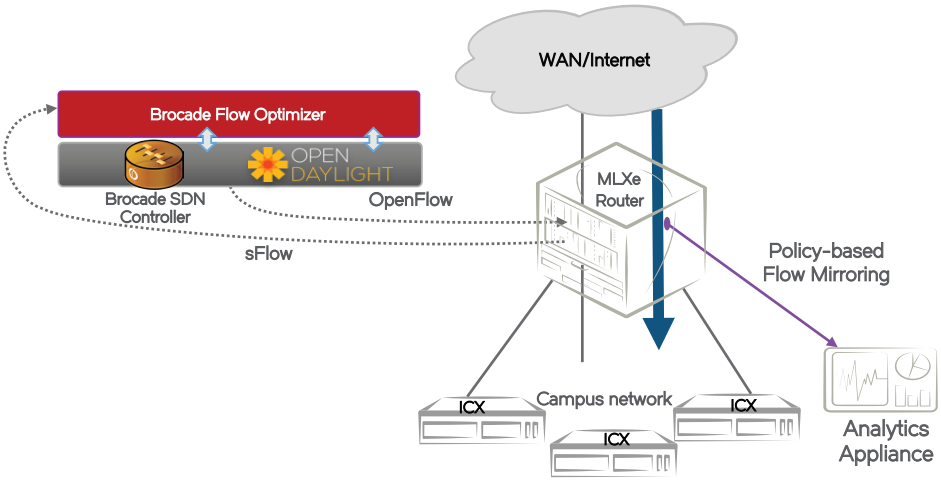

Figure 5. Brocade Flow Optimizer-Flow-based Application Traffic Mirroring.

Flow-Based Application Traffic Mirroring

In this use case, customers can mirror the traffic for a given application to a separate specific port that is connected to an analytics appliance, as shown in Figure 5. The application traffic is identified by a policy profile that has been established based on, for example, source IP address and UDP/TCP ports type.

This SDN-based use case offers a significant advantage, especially as higher-speed connections such as 40 Gigabit and 100 Gigabit ports are being used more, when compared to traditional methods based on port mirroring or port span. Customers can now mirror the traffic related to a single application of interest versus the entire traffic on a given port. This reduces the traffic requirements of the analytics appliances, which in turn, reduces CapEx and OpEx, and the upfront costs that include capacity licenses. This also reduces the time needed to access very specific data.

Science DMZ

In this use case, customers can use the Brocade Flow Optimizer to identify large high-performance data traffic, typical of research environments, and quickly direct it to the intended High Performance Computing (HPC) cluster or Data Transfer Node (DTN) in a campus. As seen in Figure 6, customers increase network efficiency by reducing the time to transfer such data flows while avoiding any latency that might be induced in the

process. These large high-performance traffic flows are typically in the range of 100 Gigabit per second or higher nowadays and are considered to be trusted flows. These flows can avoid creating extra cycles in the network and can also bypass firewalls and security appliances, conserving network resources. These high-performance traffic flows can safely bypass firewalls and other security appliances, eliminating unnecessary consumption of network resources. These large trusted data flows can be received from an upstream network, such as a research network, the Internet or a cloud service provider. Using an SDN solution like the Brocade Flow Optimizer, customers can quickly match these trusted flows to existing pre-programmed traffic profiles based on certain established policies and automatically redirect them to defined destination ports to effectively bypass a firewall/security appliance. The same process can be applied to large trusted data flows being transferred from the HPC or DTN back to the upstream network, thus accelerating outbound transfers.

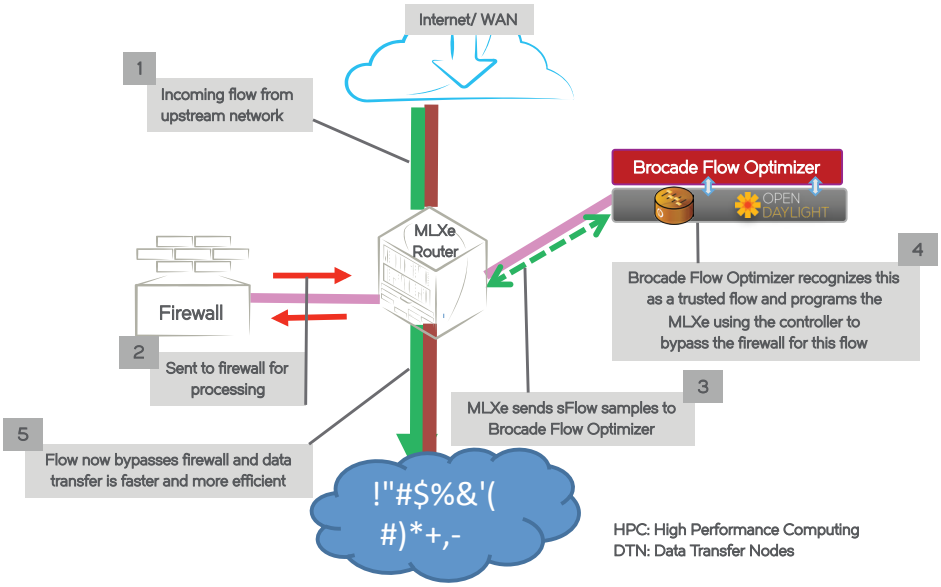

Figure 6. Brocade Flow Optimizer- Science DMZ.

Seamlessly Enabling Higher Network Performance

As demonstrated in these use cases, the Brocade Flow Optimizer application allows customers to quickly realize the benefits of SDN technology while introducing new levels of visibility, programmability, and automation. The Brocade Flow Optimizer can be seamlessly introduced in the network, enabling customers to address various network uses cases and help reduce costs while providing flexible and scalable network performance.

Learn More

Brocade partners with companies of all sizes to deliver innovative solutions that help organizations maximize the value of their most critical information. To learn more, visit www.brocade.com.

About Brocade

Brocade networking solutions help organizations transition smoothly to a world where applications and information reside anywhere. Innovative Ethernet and storage networking solutions for data center, campus, and service provider networks help reduce complexity and cost while enabling virtualization and cloud computing to increase business agility. Learn more at www.brocade.com.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

BROCADE