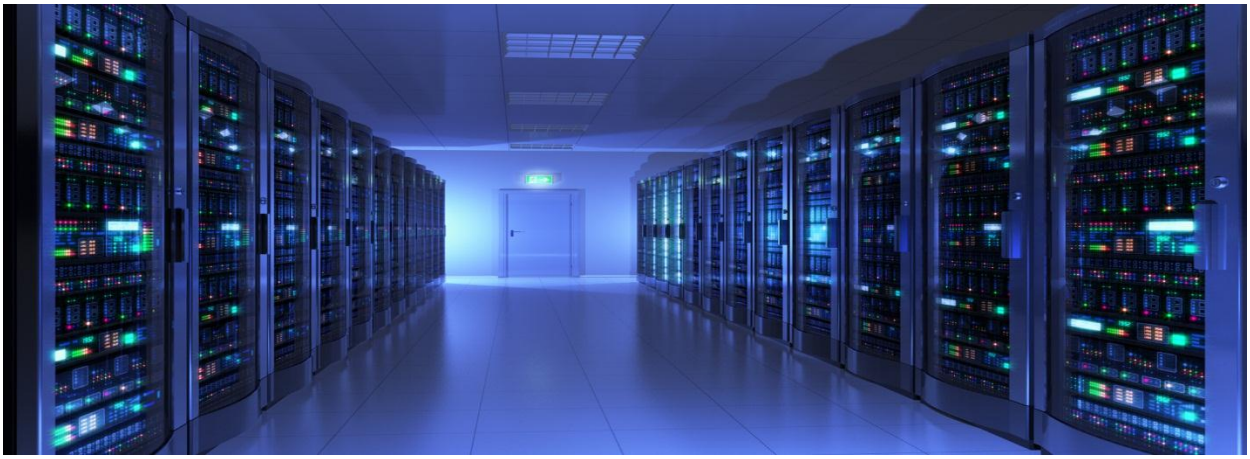


SDN ANALYTICS FOR DDOS MITIGATION

SOLVING REAL WORLD ENTERPRISE PROBLEMS TODAY

APPLICATION NOTE

Alcatel·Lucent Enterprise

SDN Analytics for DDoS Mitigation- Solving Real World Enterprise Problems Today!

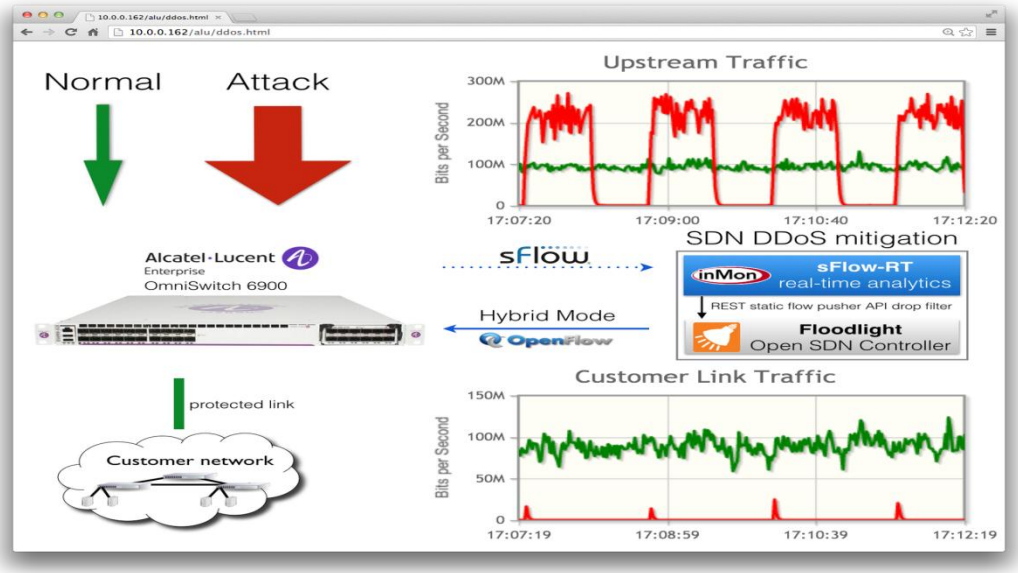
The rapid growth in data consumption, smart devices and applications is putting pressure on IT infrastructure and its security. A distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. It temporarily or indefinitely interrupts or suspends services of a host connected to the Internet. Everywhere you look, leading publications are filled with stories on the growing problem of DDoS attacks and the market opportunity for mitigation solutions, Prolexic Publishes Top 10 DDoS Attack Trends for 2013, World's largest DDoS strikes US, Europe. DDoS attacks are a growing threat in the Enterprise and need to be addressed.

The network is the bottleneck for IT being able to securely provision services and scale through automation. Traditional network architectures are static requiring significant operational resources to keep up with the demands placed on them. And, most still don't meet the business needs of controlling costs and improving agility. Enterprises need and are demanding solutions that improve operational efficiency and business agility.

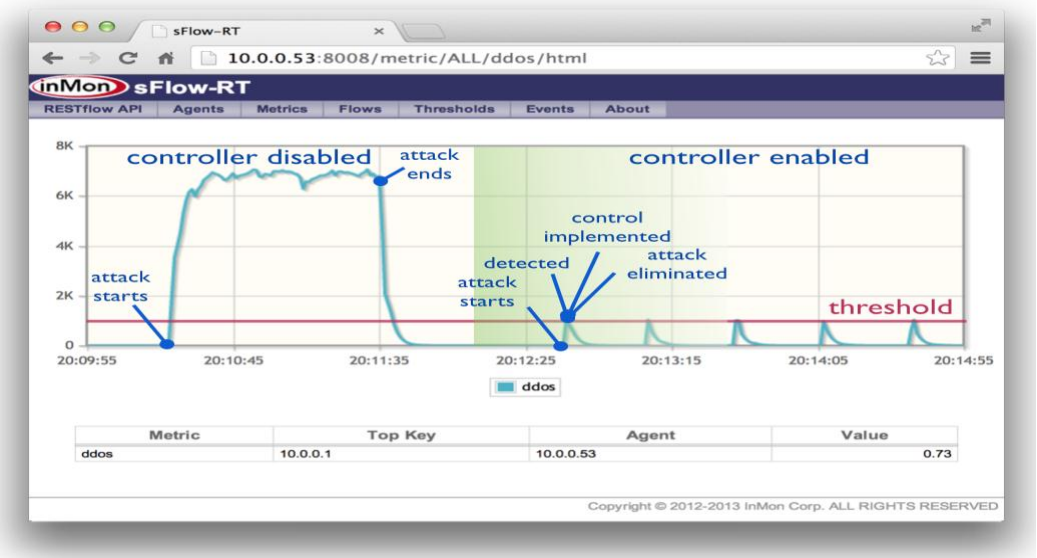
Software Defined Networks (SDN) is an industry initiative that enables the transformation of the network infrastructure from an IT perspective. The goal of SDN initiative is to virtualize network services and provide benefits that include:

- Secure, dynamic, application-tuned network provisioning and performance
- Multipath and multi-tenant networks
- Network-layer abstraction offering programmable services to ease application deployment and migration
- Evolution from vendor-specific command line interfaces (CLIs) to a generic programmable interface

The diagram below depicts the building blocks for a secure and agile Enterprise. Standard sFlow enabled on the switches and routers provides a continuous stream of measurement data to InMON sFlow-RT, which provides real-time detection and notification of DDoS attacks to the DDoS Mitigation SDN Application. The DDoS Mitigation SDN Application selects a mitigation action and instructs the SDN Controller to push the action to selected switches (for example using a standard OpenFlow rules to drop traffic associated with the DDoS attack).



The key making this solution scale is the use of hybrid port OpenFlow. By default, all traffic is handled by the switch's normal hardware switching and routing engine without any intervention from the controller. The OpenFlow rules are used to override the normal forwarding behavior for the selected flow. The solution uses an OPEN SDN Controller to leverage the standard sFlow and OpenFlow capabilities of existing network hardware to provide a scalable, automated, cost effective solution that allows Enterprise networks to effectively mitigate flood attacks.



The diagram shows that implementing traffic engineering using OpenFlow considerably cuts the time to implement controls from seconds to milliseconds.

OpenFlow is a southbound application programming interface (API) to programmatically control both virtual and physical switches. SDN controllers have a northbound API to enable service-driven orchestration of the network fabric, normally integrated with application service orchestration tools such as vCloud Director™, OpenStack™, InMON sFlow-RT, etc.

The Alcatel-Lucent OmniSwitch platform supports the OpenFlow v1.3.1 compliant agent. The agent is backwards-compatible with controllers that support OpenFlow v1.0. The platform supports the following OpenFlow modes:

- Full: All ports are managed by the controller
- Hybrid: A subset of the ports are managed by the controller and the remaining function as default AOS managed ports
- OpenFlow API mode: The port is a regular bridged port, but the controller can modify flow characteristics on these ports if required. These flow updates will be treated as remote access control list (ACL) updates.
- The ports under controller management can be split into three logical switches. Each logical switch can be managed by up to three controllers for redundancy and resiliency.

For details on the complete script please refer to sFlow blog: [OmniSwitch SDN Analytics DDoS Mitigation]

References:

http://www.itbriefcase.net/top-ddos-attack-trends-for-2013
http://www.itnews.com.au/News/372033,worlds-largest-ddos-strikes-us-europe.aspx
IDC: Worldwide DDoS Prevention Products and Services 2013-2017 Forecast
Infonetics: Global DDoS Prevention Appliances 2012-2017 Forecast

Alcatel·Lucent
Enterprise