DDOS THREAT DETECTION, ANALYSIS AND MITIGATION AT ANY SCALE

A10 Networks and FlowTraq help manage the largest and most complex DDoS attacks

Challenge:

Protecting networks requires access to detailed insight into what traffic is flowing between an organization's services and the Internet. Knowledge is power for an administrator, who needs historical and current data to scale network resources, as well as algorithms to detect anomalies that threaten service availability.

Solution:

FlowTraq provides detailed information and statistics about what's happening in the network. When network anomalies such as DDoS attacks are detected, FlowTraq interacts with A10 Thunder TPS to redirect suspect traffic for further analysis and to manage the largest and most complex DDoS attacks.

Benefits:

- FlowTraq provides deep insight at any level into your network traffic flows.
- Automated DDoS detection and mitigation easily escalates suspect traffic to A10 Networks Thunder TPS for further traffic validation and DDoS mitigation.
- Network traffic is continuously monitored and analyzed to establish peacetime baselines, without additional latency. Minimal latency when mitigation is required.

Knowledge and Power

Networks face many challenges created by the traffic they have to manage. Distributed Denial of Service (DDoS) traffic is intentionally generated to take out online services, for various motivations ranging from idealism/hacktivism to extortion or even "because they can."

For network staff, it is critical to know what traffic behavior is occurring on the network, what traffic types are involved, and where in the network these are occurring. This knowledge is used for monitoring and predicting network expansion requirements, but it is also critical for analyzing network problems.

Network problems such as DDoS attacks come in many shapes and forms. Some are well-known and easy to spot by the overwhelming packet-per-second rates and bandwidth, but stealthier "slow-and-low" or zero-day attacks are not always easy to detect until services are actually affected.

Analyzing network flow samples are an excellent way to scale the network analysis systems, as they require less packets and therefore less bandwidth yet provide deep insight, high visibility and valuable understanding of complex network infrastructures. Once traffic anomalies such as a high packet-per-second DDoS attacks are detected, the next problem is how to mitigate the attack before the services are impaired and the organization's revenue and reputation are put in jeopardy. A DDoS mitigation solution has to be able to scale with different DDoS attack types, which are often fired in parallel to maximize an attack's efficiency. These multi-vector DDoS attacks use network- or infrastructure-layer attacks such as SYN floods and more sophisticated, lower volume application-layer attacks. Because of their stateful nature, classic security solutions such as firewalls and intrusion detection system (IDS) devices are quickly overwhelmed with the DDoS assault, and a dedicated DDoS mitigation solution that is able to provide network-wide protection from multi-vector attacks is required.

A10 and FlowTraq

A10 Networks and FlowTraq have partnered to provide a flexible, scalable and affordable solution for flow-based network insight, analysis and DDoS mitigation. As traffic traverses the network, it is being watched by FlowTraq, which receives flow samples from routers in various parts of the network and determines traffic baselines. Once a network anomaly is detected, FlowTraq, using A10's RESTful API interface, tells A10 Networks® Thunder TPS™ line of Threat Protection Systems what protected object is under attack, and what mitigation action is required. The A10 Thunder TPS device, in turn, instructs the network to redirect the malicious traffic to the Thunder TPS. The traffic now gets cleaned of the malicious components, and legitimate traffic is forwarded to the target server.

FLOWTRAQ

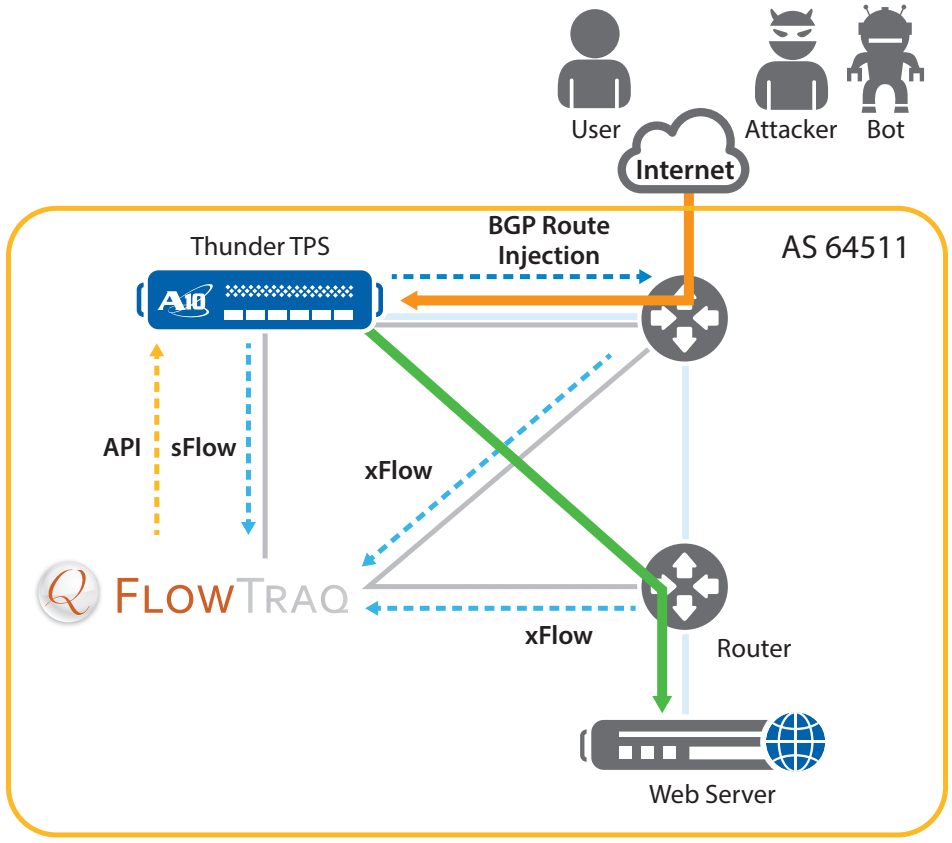

Figure 1: Thunder TPS and FlowTraq interaction

Ease of Administration and Scale

FlowTraq allows network administrators as well as network security staff to analyze network traffic in depth and define policies that react to certain traffic types and traffic rates. FlowTraq servers seamlessly scale up with network traffic rates and the inherent flow sample rates. The GUI provides an intuitive interface to display the various traffic patterns that FlowTraq can determine.

FlowTraq automatically creates a baseline for destination IP addresses. Over time, FlowTraq identifies the regular traffic patterns for a destination and determines when traffic patterns are out of the ordinary. Once anomalous traffic is detected, Thunder TPS can then be interjected and apply a mitigation policy to block the malicious traffic. Static traffic rate thresholds can be manually configured for users who want more control.

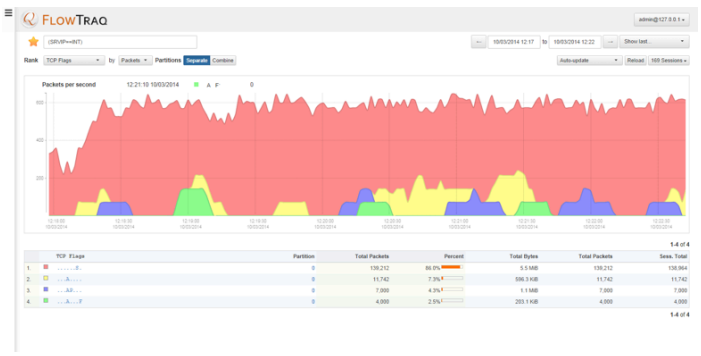

Figure 2: SYN flood attack

Select Thunder TPS models feature A10's Thunder Security and Policy Engine (SPE) for hardware accelerated traffic processing. With hardware acceleration, Thunder TPS is able to mitigate more than 60 attack vectors in hardware, reserving the powerful CPUs for more complex tasks. This allows Thunder TPS to scale under the heaviest of multi-vector attacks.

Features and Benefits

With the integrated FlowTraq and Thunder TPS solution, your network traffic patterns are analyzed, can be accessed and presented to gain insight and provide protection against malicious DDoS attacks. Deploying Thunder TPS with FlowTraq provides:

- Deep traffic analysis: FlowTraq provides insight at any level of your network traffic flows.
- Automated detection and mitigation: Easily escalate suspect traffic to the Thunder TPS for further traffic validation and DDoS mitigation. FlowTraq analyzes normal network patterns and automatically determines when an anomaly is occurring. Thunder TPS quickly eliminates DDoS traffic, whether volumetric or targeted on the application layer or both.
- Optimal latency: With FlowTraq and Thunder TPS, a dynamic and reactive deployment model can be deployed. FlowTraq continuously monitors the traffic and establishes baselines, and provides rapid detection of anomalies with no added latency. Thunder TPS can dynamically be inserted when necessary, adding only minimal latency.

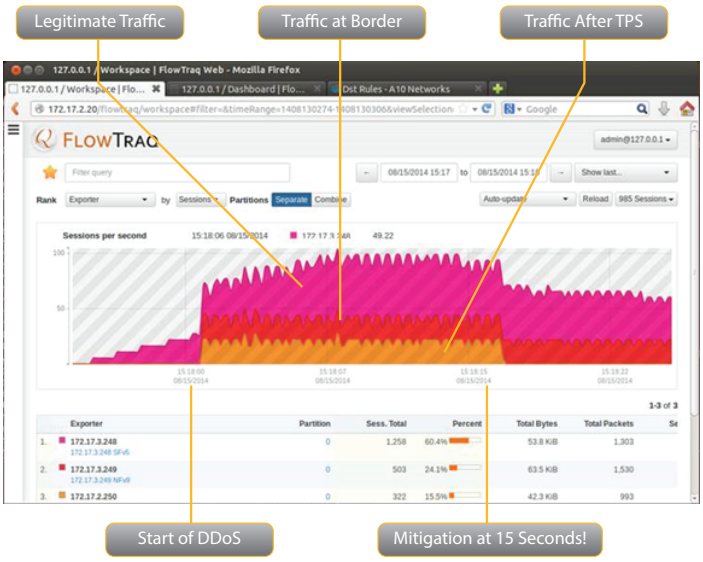

Figure 3: DDoS detection and mitigation

About FlowTraq

Founded in 2004, FlowTraq develops and markets software solutions that monitor and analyze network security and performance to provide deep insight, high visibility and valuable understanding of complex network infrastructures. With FlowTraq, users gain an unprecedented level of network situational awareness that facilitates fast and easy monitoring, quick security analysis and complete forensic recall of any traffic that crosses their network, thus reducing organizational risk. FlowTraq software solutions include FlowTraq, FlowTraqCloud and FlowExporter. FlowTraq has over 2,600 customers worldwide, including Fortune 500 companies, ISPs, Managed Service Providers, government, schools, and universities. FlowTraq is privately held and headquartered in New Hampshire. For more information, visit http://www.flowtraq.com/corporate/.

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-SB-19129-EN-01
Nov 2014

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Hong Kong
HongKong@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.