May 14, 2018

TRAFFIC REDIRECTION WITH DISTRIBUTED DENIAL OF SERVICE SEGMENT IDENTIFIERS

Robert Barton

Jerome Henry

Siva Sivabalan

TRAFFIC REDIRECTION WITH DISTRIBUTED DENIAL OF SERVICE SEGMENT IDENTIFIERS

AUTHORS:
Robert Barton
Jerome Henry
Siva Sivabalan

ABSTRACT

Distributed Denial of Service (DDoS) information is extended to a network Path Computation Element (PCE). The PCE uses a network function Segment Identifier (SID), referred to herein as a DDoS SID, imposed on the edge routers by the PCE, to identify potentially suspicious DDoS traffic. The DDoS SID is used in Segment Routing (SR) routers to direct suspicious traffic to nearby or specially optimized DDoS scrubbing engines so that traffic may be cleaned. Other traffic flows proceed unchanged through the network.

DETAILED DESCRIPTION

Distributed Denial of Service (DDoS) attacks are difficult to solve through traditional methods (e.g., Border Gateway Protocol (BGP) black holing, Access Control Lists (ACLs), rate limiters, etc.). These methods tend to filter out both legitimate traffic and the offending DDoS traffic at the same time. New high performance in line traffic scrubbers have appeared on the market that attempt to better filter traffic by removing the offending traffic and forwarding the legitimate traffic. However, filters still present the limitation of redirecting all traffic intended for a potential DDoS victim to the scrubber. With the emergence of new routing architectures, in particular, Segment Routing, network automation and Network Functions Virtualization (NFV) capabilities may greatly enhance the efficiency of redirection, by building on the ability to quickly identify and remove offending DDoS flows.

In one example, a DDoS detection system detects that a DDoS attack is occurring. The DDoS detection system may be on-premise or otherwise, and may be in a firewall, NetFlow analyzer, etc.). After detection, the attack is reported to a cloud-based central DDoS prevention controller. At this point, the DDoS prevention controller communicates

details of the attack to the SR Path Computation Element (PCE). This may be accomplished through normal SR PCE communication models such as PCE Protocol (PCEP).

After receiving DDoS flow information, the PCE gains insight into the attack vector (e.g., destination IP, destination port, etc.), along with valuable flow and application-layer information.

The PCE then forwards an identifier for the suspicious traffic to the SR edge routers, and instructs them to impose a DDoS SID. The DDoS SID is embedded in the packet header as part of the overall SID label stack. As the packet passes through the network, they are observed by transit routers as "DDoS suspicious".

The DDoS SID is not a simple packet forwarding SID label. Instead, the DDoS SID represents a network function in which the function is DDoS scrubbing. When an SR router receives a packet with the DDoS SID in the label stack, the router performs a lookup in its binding SID table for instructions based on the DDoS SID. The binding SID table is a set of instructions for network function SIDs that is part of the SR process in every router. In this case, the table includes instructions indicating that the router should forward the "DDoS suspicious" traffic for further investigation and cleaning. This traffic may be forwarded the closest scrubber.

The intention is to identify the offending traffic streams at the entry points of the network and then use SR to steer (via SR Traffic Engineering) only the offending flows to a nearby or optimized traffic scrubber for deeper analysis. Here, the offending traffic will be removed and the good traffic will be kept. There may be multiple scrubbers in different locations. Flagging traffic as suspicious with the DDoS SID at the entry points of the network enables redirecting that traffic to the closest scrubber, thus load balancing traffic across scrubbers (as DDoS traffic typically is sourced from multiple addresses, and therefore enters the network through multiple points). Redirection may also occur before the suspicious traffic reaches the attacked segment, thus limiting the attack surface.

The combination of PCE traffic engineering and SR binding SIDs on the router may facilitate the DDoS SID function. At the entry point of the network, it is not possible to identify with absolute certainty whether a particular traffic flow is part of the DDoS attack, because the DDoS traffic may be mixed with clean traffic. However, using SR, a packet may initially be labeled as DDoS suspicious (meaning it requires further investigation

through an in line traffic scrubber). This information may then be distributed, and associated instructions provided to the SR routers throughout the network.

Figure 1 below illustrates an example overview diagram.

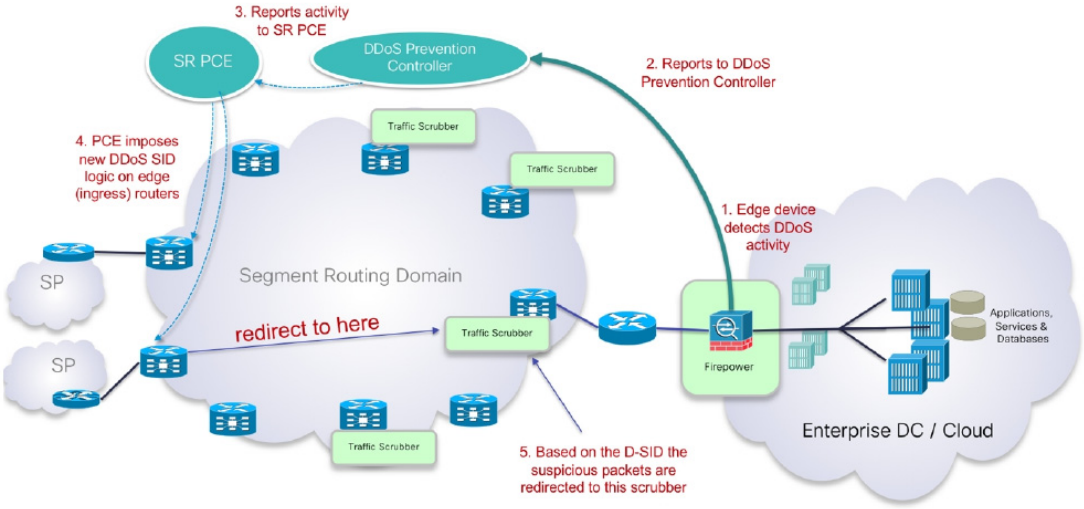

Figure 1

These techniques may use existing methods to identify suspicious DDoS traffic and communicate to a network programming device. However, these techniques may also involve one or more of the following operations: (1) inserting a DDoS SID, which identifies the flow as suspicious and enables redirecting the flow towards a scrubber; (2) using the DDoS SID to invoke NFV capabilities in the router, where the scrubber is the virtualized function; and (3) re-engineering the cleaned traffic once it emerges from the scrubber (e.g., after the traffic passes through the scrubber, the DDoS SID may be removed from the cleaned traffic and forwarded to the intended destination).

These techniques enable imposing a unique “DDoS Suspicious” SID (DDoS SID) into the label stack, in a place of the user’s choosing. Concretely, the DDoS SID may be programmed into the routers by the PCE at an optimal position in the label stack (not necessarily the top or bottom of the stack). The purpose of this is to redirect, or traffic engineer, the DDoS traffic to the desired destination (e.g., the scrubber, which is a “network function”).

Unlike Security Group Tags (SGTs), which only involve inserting one label into the header to identify a group (which mechanically translates into “must be filtered”), the

SID stack is used to both steer the traffic programmatically toward a network function, as well as to identify the traffic as "DDoS suspicious". That network function may be "scrub," but the function may also be different, and may also result in different functions on different SR routers (e.g. "redirect to scrub," "drop," "take secondary path to same destination," etc.). By contrast, SGTs/TrustSec cannot apply a dynamically differentiated network function based solely on a given label.

Additionally, when a packet arrives at a midpoint node, the router observes the DDoS SID in the label stack and invokes the binding SID capability within the router. Instead of simply forwarding the packet to the next segment, the binding-SID permits identifying this packet as requiring a specialized network function (e.g., the scrubber). In this case, the router does a lookup in the binding SID table and then forwards the packet to a nearby DDoS scrubber. Furthermore, the DDoS SID imposed by the PCE allows the router to intelligently choose the optimal scrubber and the path to arrive at the scrubber. For example, as load increases, a given SR may redirect all suspicious traffic to a given scrubber or start directing to a second scrubber, reacting to the same label but an increase traffic load. SGTs are unable to apply such progressive (software-based) traffic engineering functions.

In summary, DDoS information is extended to a network PCE. The PCE uses a network function SID, referred to herein as a DDoS SID, imposed on the edge routers by the PCE, and used to identify potentially suspicious DDoS traffic. The DDoS SID is used in SR routers to direct suspicious traffic to nearby or specially optimized DDoS scrubbing engines so that traffic may be cleaned. Other traffic flows proceed unchanged through the network.