March 2022

METHOD TO COUNTER DISTRIBUTED DENIAL OF SERVICE ATTACK IN SEGMENT ROUTING USING HYPERLEDGER

NIRANJAN M M

METHOD TO COUNTER DISTRIBUTED DENIAL OF SERVICE ATTACK IN SEGMENT ROUTING USING HYPERLEDGER

AUTHOR:
NIRANJAN M M

ABSTRACT

Distributed Denial of Service (DDoS) attacks are difficult to solve through traditional methods. Traditional methods tend to filter out both legitimate traffic and the offending DDoS traffic at the same time. There are techniques which filter traffic by removing the offending traffic and forwarding the legitimate traffic by using high performance in-line traffic policers. Here, all the traffic intended for a potential DDoS victim need to be processed. The techniques presented herein propose method to handle DDoS attack using Hyperledger where-in the Firewall/NetFlow analyser/Edge Router detect the DDoS attack and report back to the "source" about the attack vector (e.g., destination IP, source IP, destination port etc.,) along with valuable flow and application layer information. Also map attack vector to the Distribution Denial of Service Segmentation ID (DDoS SID), so that SR router at the source itself identify the offending traffic stream and flag as suspicious with the DDoS SID at the entry points of the network. Based on the DDoS SID, the traffic would be redirected to traffic policer for further processing. Other traffic flows proceed unchanged through the network. To reduce false positives (i.e., initially suspicious traffic is labelled with DDoS SID, but after passing through the "traffic policer", found to be legitimate traffic flow.) "Traffic policer" updates DDoS traffic statistics to the Hyperledger and periodically Firewall/Edge Router learn and adopt to remove legitimate traffic being labelling with DDoS SID. As redirection and filtering of such DDoS traffic occurs very early at the entry point, i.e., before suspicious traffic reaches the attack segment, hence limiting the attack surface.

DETAILED DESCRIPTION

Distributed Denial of Service (DDoS) attacks are difficult to solve through traditional methods. Traditional methods tend to filter out both legitimate traffic and the offending DDoS traffic at the same time. There are techniques which filter traffic by removing the offending traffic and forwarding the legitimate traffic by using high performance in-line traffic policers. Here, all the traffic intended for a potential DDoS victim need to be processed. Existing techniques uses centralised approach, which causes single point of failure.

With the emergence of new routing architectures (i.e., Segment Routing, network automation and Network Functions Virtualization [NFV]) and new technologies (such as Blockchain, Hyperledger), can greatly enhance the efficiency of filter and removing DDoS flows by building the ability to quickly identify using distributed approach (using Hyperledger) and marking the suspicious DDoS traffic flow by DDoS SID.

The techniques presented herein propose method to handle DDoS attack using Hyperledger where-in the Firewall/NetFlow analyser/Edge Router detect the DDoS attack and report back to the "source" about the attack vector (e.g., destination IP, source IP, destination port etc.,) along with valuable flow and application layer information. Also map attack vector to the Distribution Denial of Service Segmentation ID (DDoS SID), so that SR router at the source itself identify the offending traffic stream and flag as suspicious with the DDoS SID at the entry points of the network. Based on the DDoS SID, the traffic would be redirected to traffic policer for further processing. Other traffic flows proceed unchanged through the network.

To reduce false positives (i.e., initially suspicious traffic is labelled with DDoS SID, but after passing through the "traffic policer", found to be legitimate traffic flow.) "Traffic policer" updates DDoS traffic statistics (e.g., drop count) to the Hyperledger. Further, Firewall/Edge Router continuously learn and adopt to remove legitimate traffic being labelling with DDoS SID.
As redirection and filtering of such DDoS traffic occurs very early at the entry point, i.e., before suspicious traffic reaches the attack segment, hence limiting the attack surface.

The techniques presented herein divided into mainly two feedback mechanisms:
Feedback Mechanism-1:

1. Firewall running on the Edge (on-prime/enterprise) detect DDoS activity and identify attack vector where DDoS is prominent. Firewall update attack vector (source IP, destination IP, port etc.,) used to identify the DDoS activity to the Hyperledger.
2. Firewall, PCE and all the SR routers in the deployment would register with the Hyperledger and perform authentication before accessing, as it is authenticated private blockchain.
3. Attack vector, valuable flow and application information will be stored into the Hyperledger (private Blockchain).
4. PCE fetch attack vector (source IP, destination IP, port etc.,), valuable flow and application information used to identify the DDoS activity from the Hyperledger and derive DDoS SID. Also, PCE update derived DDoS SID to the Hyperledger.
5. PCE impose DDoS SID logic for the suspicious traffic based on the attack vector, flow, and application information to the SR router.
6. Based on the DDoS SID, the suspicious packets are redirected to SR router having traffic policer functionality (which is like BGP blackhole filtering).
7. Traffic policer applies the policies (viz., rate limiting, etc.,) and send the cleaned traffic to the next hop in the segmentation routing domain.

Figure-1 describe feedback mechanism-1 to handle DDoS traffic in Segment Routing using Hyperledger.

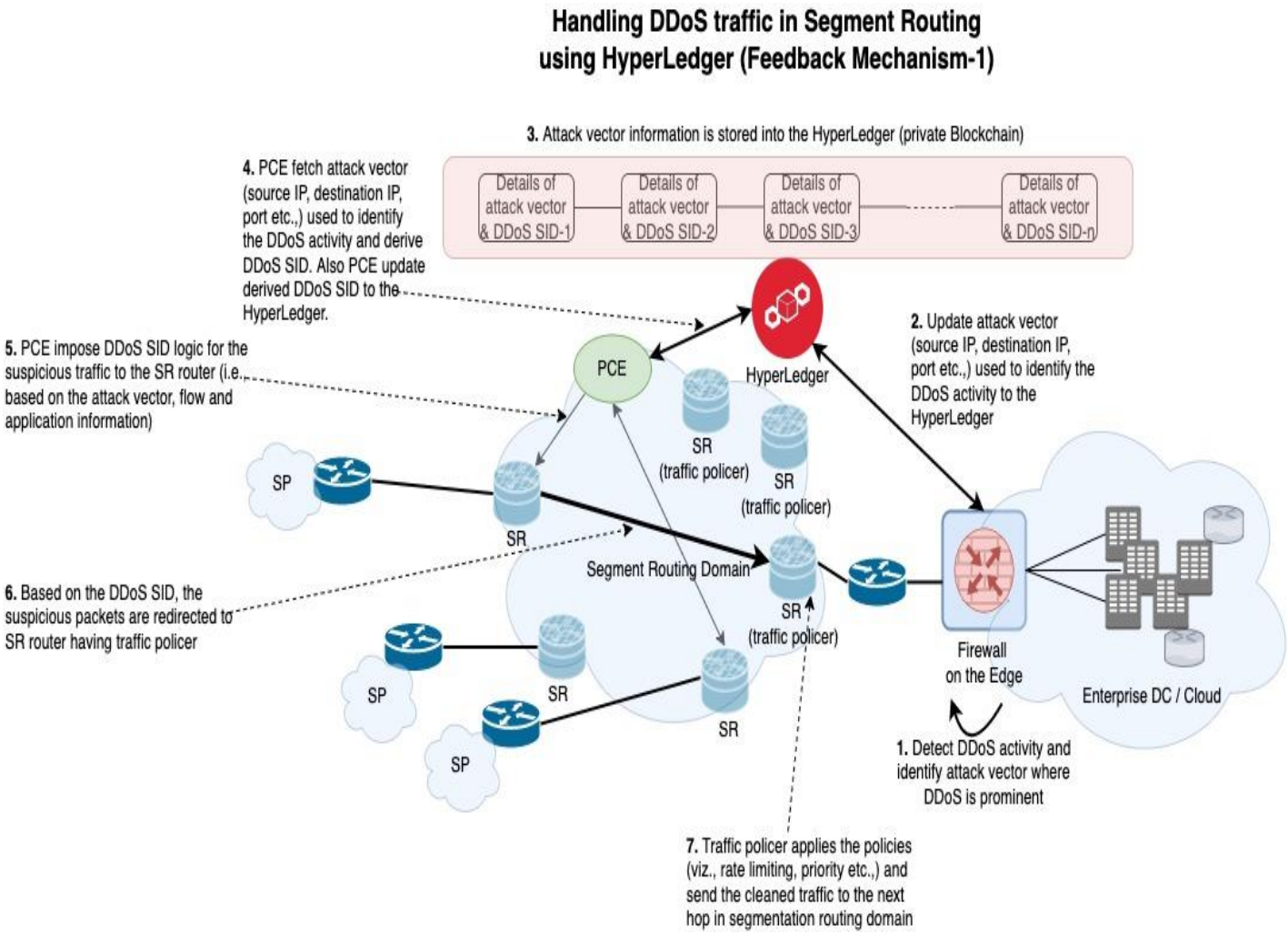

Figure-1

Feedback Mechanism-2:

8. Periodically, traffic policer updates the Hyperledger with DDoS traffic statistics such as total rate limited packet count (drop count, burst traffic etc.,) and mark whether the suspicious traffic is really a DDoS traffic or a false positive (i.e., legitimate traffic wrongly marked).
9. Periodically Firewall on the enterprise edge fetch the attack vector details along with information updated by one or more traffic policer for that attack vector.
10. Firewall re-run the logic on attack vector, flow, and application information.
11. Firewall update the attack vector status along with new attack vector to the Hyperledger.
12. Updated attack vector information is stored to the private/permission blockchain (Hyperledger).
13. Later PCE derive DDoS SID based on new attack vector.
14. PCE impose new DDoS SID Logic.

Figure-2 describe feedback mechanism-2 to handle DDoS traffic in Segment Routing using Hyperledger.

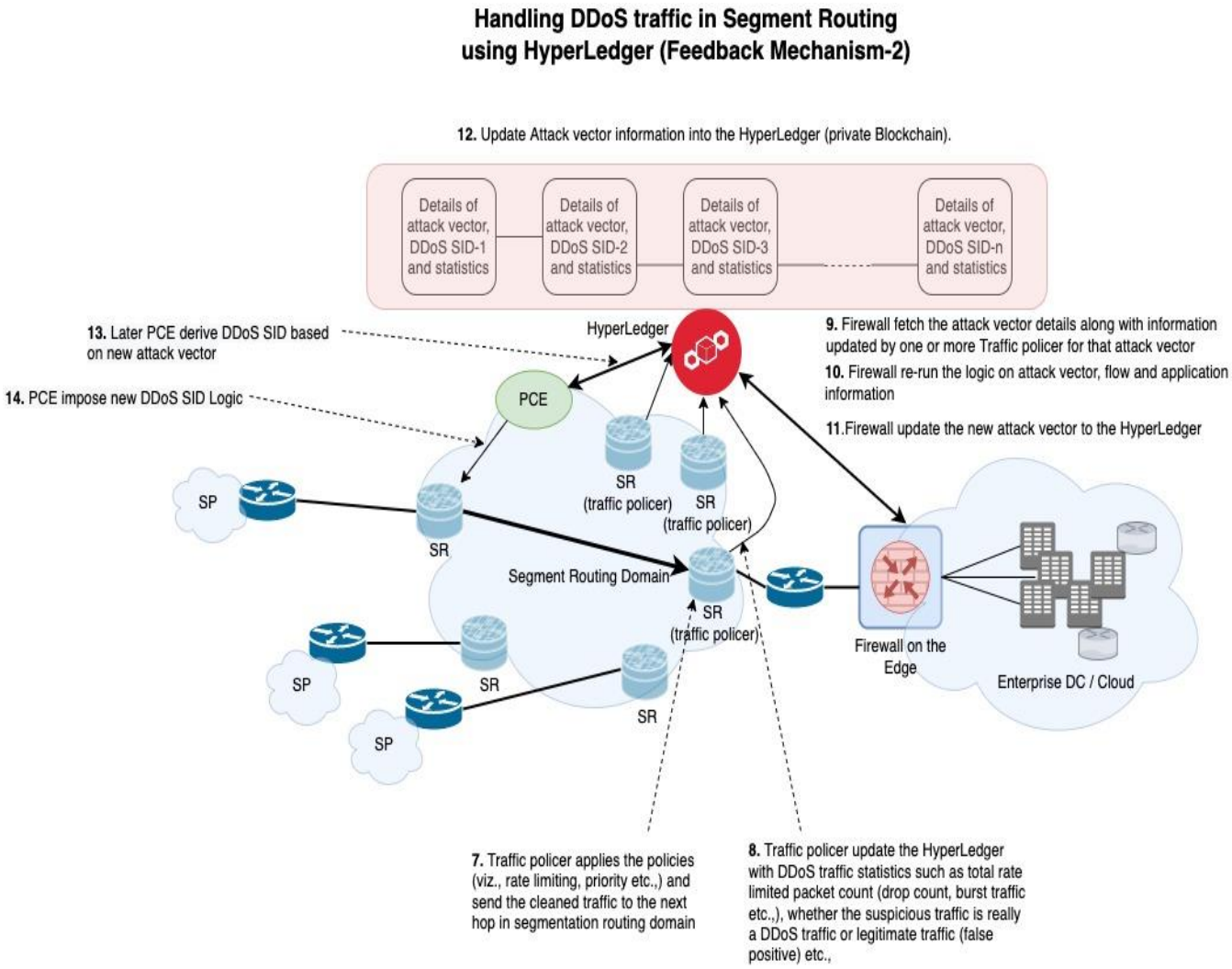

Figure-2

In summary, the techniques presented herein propose secure and distributed method to combat DDoS attack in Segment Routing deployments. Moreover, the method counters the DDoS attack very early at the entry point, i.e., before suspicious traffic reaches the attack segment, hence limiting the attack surface. Additionally, the method uses two closed loop feedback approach to reduce the false positives in marking suspicious traffic with DDoS SID.