ABSTRACT

GONÇALVES, D. S. M. *Botnet Attack Protection System using Software Defined Networks*. 2020. 63 f. Dissertação (Mestrado em Engenharia Eletrônica) – Faculdade de Engenharia, Universidade do Estado do Rio de Janeiro, Rio de Janeiro,
2020.

Denial of service attacks are growing every year requiring financial and technological investments by corporations to prevent damage to their services provided on the Internet. In general, protection systems against these attacks are implemented using expensive equipment that processes a high volume of traffic. In addition, some companies offer malicious traffic handling services to other autonomous systems on the Internet that are also expensive. This dissertation proposes a protection system against HTTP flood botnet attacks based on SDN (Software Defined Networking) network technology using the collaboration of other ASs. These ASs use SDN networks controlled through a VPN by the protection system of the web server targeted by the attacks. Another implemented VPN is used to allow collaborating ASs to send requests directly to the web server that is protected by the original system. The requests destined to the web server with the final service are answered by the system and receive a redirection to the real destination of the protected application. Through the implementation of the system with SDN, each request will have a permissive flow written on a virtual switch that gives access to the web server. Since requests from botnets will not access the actual destination because they do not follow the received redirect, only requests from legitimate clients will reach the protected server. This allows the system to differentiate attacking IPs from legitimate client IPs. In this way, attackers are blocked through blocking flows inserted into the system's virtual input switch. The proposed system was implemented and performance evaluations were carried out. The results obtained show gradual reductions in CPU consumption of the local controller server, during an attack, as collaborating ASs are added to the system. With six collaborating ASs and the system under attack, a drop in CPU consumption of the local controller server of 65.32%, a drop in latency perceived by customers from 6 s to approximately 400 ms and a drop in in 78% web server CPU consumption.

Keywords: SDN. Attacks. Protection.