ĐỀ XUẤT GIẢI PHÁP PHÁT HIỆN VÀ GIẢM THIỂU TÁC HẠI TẤN CÔNG DDOS BẰNG PHƯƠNG PHÁP THỐNG KÊ DỰA TRÊN KỸ THUẬT MẠNG CẤU HÌNH BỞI PHẦN MỀM SDN

A PROPOSAL FOR DETECTION AND MITIGATION OF DDOS ATTACKS USING STATISTICAL METHOD BASED ON SOFTWARE DEFINED NETWORKING

Tác giả: *Đặng Văn Tuyên, Trương Thu Hương, Nguyễn Tài Hưng*

Tóm tắt bằng tiếng Việt:

Trong bài báo này, chúng tôi đề xuất một giải pháp phát hiện và giảm thiểu tác hại tấn công DDoS dựa trên kỹ thuật mạng cấu hình bằng phần mềm SDN và chuẩn giao thức Openflow. Một số tham số thống kê được lựa chọn và thu thập định kỳ từ các flow entries trên OF switch dùng cho tính toán để phát hiện tấn công. Khi phát hiện có tấn công xảy ra, cơ chế điều khiển từ controller tới OF switch được sử dụng để lọc bỏ các gói tin nghi ngờ. Quá trình được thực hiện một cách tự động bằng phần mềm với thuật toán đơn giản, thực thi trực tuyến, chỉ sử dụng các tham số thống kê từ OF switch. Kết quả phân tích đánh giá hiệu năng cho thấy giải pháp cho tỷ lệ phát hiện (DR) cao (hơn 95%) với tỷ lệ dương tính giả (FPR) thấp (xấp xỉ 4%).

Từ khóa: DDoS; phát hiện tấn công DDoS; giảm thiểu tấn công; kỹ thuật mạng cấu hình bởi phần mềm; SDN; Openflow

Tóm tắt bằng tiếng Anh:

In this paper, we propose a measure for detection and mitigation of DDoS attacks based on Software Defined Networking (SDN) and Openflow protocol. Some statistical parameters which are selected and periodically gathered from flow entries on OF switches are used for calculating to detect attacks. If an attack is detected, the control mechanism of SDN is used to allow the controller to order the OF switch to drop suspected packets. The process is operated automatically and on the fly by software with simple and effective algorithms on statistical parameters taken from OF switches. The result of analysis and assessment of effectiveness shows that the solution could give a high detection rate (over 95%) with a relatively low false positive rate (approximately 4%).

Key words: DDoS; DDoS attack detection; attack mitigation; Software Defined Netwoking, SDN; Openflow.