BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 923 /QĐ-BTTTT	*Hà Nội, ngày 20 tháng 5 năm 2022*

QUYẾT ĐỊNH
Ban hành Yêu cầu kỹ thuật cơ bản đối với sản phẩm Phòng, chống tấn công từ chối dịch vụ

BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Theo đề nghị của Cục trưởng Cục An toàn thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Yêu cầu kỹ thuật cơ bản đối với sản phẩm Phòng, chống tấn công từ chối dịch vụ (Anti-DDoS).

Điều 2. Khuyến nghị cơ quan, tổ chức nghiên cứu, phát triển, lựa chọn, sử dụng sản phẩm Anti-DDoS đáp ứng các yêu cầu kỹ thuật cơ bản theo Điều 1 Quyết định này.

Điều 3. Cục An toàn thông tin chủ trì, phối hợp với các cơ quan, tổ chức liên quan hướng dẫn việc áp dụng các yêu cầu trong Yêu cầu kỹ thuật cơ bản đối với sản phẩm Anti-DDoS tại Điều 1 Quyết định này.

Điều 4. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 5. Chánh Văn phòng, Cục trưởng Cục An toàn thông tin, Thủ trưởng các đơn vị thuộc Bộ, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 5;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Cổng Thông tin điện tử của Bộ;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Huy Dũng

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

YÊU CẦU KỸ THUẬT CƠ BẢN ĐỐI VỚI SẢN PHẨM PHÒNG, CHỐNG TẤN CÔNG TỪ CHỐI DỊCH VỤ

(Kèm theo Quyết định số 923 /QĐ-BTTTT ngày 20 tháng 5 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông)

I. THÔNG TIN CHUNG

1. Phạm vi áp dụng

Tài liệu này mô tả các yêu cầu kỹ thuật cơ bản đối với sản phẩm Phòng, chống tấn công từ chối dịch vụ (Anti-DDoS). Tài liệu bao gồm các nhóm yêu cầu: Yêu cầu về tài liệu, Yêu cầu về quản trị hệ thống, Yêu cầu về kiểm soát lỗi, Yêu cầu về log, Yêu cầu về hiệu năng xử lý, Yêu cầu về khả năng bảo vệ, Yêu cầu về cảnh báo, Yêu cầu về giám sát, Yêu cầu về tự động hóa.

2. Đối tượng áp dụng

Các cơ quan, tổ chức có liên quan đến hoạt động nghiên cứu, phát triển, đánh giá, lựa chọn sản phẩm Anti-DDoS khi đưa vào sử dụng trong các hệ thống thông tin.

3. Khái niệm và thuật ngữ

Trong tài liệu này các khái niệm và thuật ngữ được hiểu như sau:

3.1. Nhật ký hệ thống (Log)

Sự kiện an toàn thông tin được hệ thống ghi lại, liên quan đến trạng thái hoạt động, thông báo, cảnh báo, sự cố, cuộc tấn công, thông tin về các mối đe dọa thu thập được và các thông tin khác liên quan đến hoạt động của hệ thống (nếu có).

3.2. Gói tin (Packet)

Gói tin là một đơn vị của dữ liệu được chuẩn hóa theo các giao thức mạng, được sử dụng để gửi, nhận thông tin giữa thiết bị nguồn và đích trên mạng.

3.3. Danh sách kiểm soát truy cập (Access Control List - ACL)

Danh sách kiểm soát truy cập (ACL) là chính sách được thiết lập trên thiết bị, theo thứ tự ưu tiên để xác định hành động của thiết bị (cho phép/chặn) đối với mỗi gói tin được xử lý bởi thiết bị phục vụ phòng, chống tấn công từ chối dịch vụ.

3.4. Tấn công từ chối dịch vụ phân tán (Distributed Denial of Service - DDoS)

Tấn công từ chối dịch vụ phân tán là một loại hình tấn công mạng nhằm làm mất tính khả dụng của hệ thống, từ nhiều nguồn tấn công phân tán khác nhau.

3.5. Cảnh báo (Alert)

Sự kiện an toàn thông tin được thu thập từ các thiết bị/nền tảng tích hợp.

3.6. Độ trễ (Latency)

Độ trễ là khoảng thời gian thiết bị cần để xử lý gói tin từ khi nhận cho đến khi đưa ra hành động chặn/cho phép đối với gói tin được xử lý.

3.7. Định tuyến qua bộ lọc (Route)

Định tuyến qua bộ lọc là việc điều hướng lưu lượng mạng qua một hệ thống trung gian thông qua cơ chế định tuyến để chặn/giảm thiểu lưu lượng tấn công.

3.8. Khôi phục (Rollback)

Là việc khôi phục lại chính sách định tuyến ban đầu trước khi thực hiện định tuyến qua bộ lọc.

II. YÊU CẦU CƠ BẢN

1. Yêu cầu về tài liệu

Anti-DDoS có tài liệu bao gồm các nội dung sau:

a) Hướng dẫn triển khai và thiết lập cấu hình;

b) Hướng dẫn sử dụng và quản trị.

2. Yêu cầu về quản trị hệ thống

2.1. Quản lý vận hành

Anti-DDoS cho phép quản lý vận hành đáp ứng các yêu cầu sau:

a) Cho phép thiết lập, thay đổi, áp dụng thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình tập danh sách kiểm soát truy cập;

b) Cho phép thiết lập thời gian hệ thống thủ công hoặc được cập nhật tự động;

c) Cho phép thay đổi thời gian duy trì phiên kết nối;

d) Cho phép đăng xuất tài khoản người dùng mà phiên kết nối còn hiệu lực.

2.2. Quản lý xác thực và phân quyền

Anti-DDoS cho phép quản lý cấu hình tài khoản xác thực và phân quyền

người dùng đáp ứng các yêu cầu sau:

a) Hỗ trợ phương thức xác thực bằng tài khoản - mật khẩu;

b) Hỗ trợ phân nhóm tài khoản tối thiểu theo 02 nhóm là quản trị viên và người dùng thường với những quyền hạn cụ thể đối với từng nhóm.

2.3. Quản lý báo cáo

Anti-DDoS cho phép quản lý báo cáo thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép tạo mới theo thời gian muốn xuất báo cáo;

b) Cho phép tải về báo cáo theo chu kỳ thời gian.

3. Yêu cầu về kiểm soát lỗi

3.1. Bảo vệ cấu hình

Trong trường hợp Anti-DDoS phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), Anti-DDoS đảm bảo cấu hình hệ thống đang được áp dụng phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp.

3.2. Bảo vệ dữ liệu log

Trong trường hợp Anti-DDoS phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), Anti-DDoS đảm bảo dữ liệu log đã được lưu lại phải không bị thay đổi trong lần khởi động kế tiếp.

3.3. Đồng bộ thời gian hệ thống

Trong trường hợp Anti-DDoS phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), Anti-DDoS đảm bảo thời gian hệ thống phải được đồng bộ tự động đến thời điểm hiện tại.

3.4. Khả năng chịu lỗi vận hành

Trong trường hợp Anti-DDoS gặp lỗi trong quá trình thực thi ACL mà không thể tự động khắc phục được, Anti-DDoS phải cho phép tự động kích hoạt chức năng bỏ qua kiểm soát và cho phép quản trị viên kích hoạt thủ công chức năng này.

4. Yêu cầu về log

4.1. Log quản trị hệ thống

a) Anti-DDoS cho phép ghi log quản trị hệ thống về các loại sự kiện sau:

i. Thay đổi ACL của hệ thống cho từng địa chỉ IP riêng biệt;

ii. Thay đổi về route/rollback một địa chỉ IP ra khỏi hệ thống;

iii. Thông tin kết quả lệnh tương tác với bộ định tuyến trên mạng lưới để route/rollback hệ thống.

b) Anti-DDoS cho phép ghi log quản trị hệ thống có các trường thông tin sau:

i. Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây);

ii. Định danh của tác nhân thực hiện quản trị hệ thống (ví dụ: tài khoản người dùng, tên hệ thống, …);

iii. Định danh của đối tượng tác động (địa chỉ IP bị tác động);

iv. Thông tin chi tiết về các thay đổi cấu hình hệ thống bởi người quản trị (ví dụ: danh sách ACL bị thay đổi);

v. Kết quả thực hiện việc thay đổi cấu hình hệ thống bởi người quản trị (thành công hoặc thất bại).

4.2. Định dạng log

Anti-DDoS cho phép chuẩn hóa log theo tối thiểu 01 định dạng đã được định nghĩa trước để truyền dữ liệu log cho các phần mềm quản lý, phân tích, điều tra log.

4.3. Quản lý log

Anti-DDoS cho phép quản lý log đáp ứng các yêu cầu sau:

a) Cho phép tìm kiếm log theo từ khóa theo thời gian và theo đối tượng;

b) Phân chia log thành tối thiểu 02 nhóm:

i. Log hành vi tương tác người dùng;

ii. Log hành vi tương tác của Anti-DDoS với các thiết bị mạng khác.

5. Yêu cầu về hiệu năng xử lý

Anti-DDoS được triển khai thỏa mãn cấu hình tối thiểu theo hướng dẫn cài đặt và thiết lập cấu hình của nhà sản xuất phải đảm bảo đáp ứng các yêu cầu sau:

5.1. Độ trễ khi đi qua bộ lọc

Anti-DDoS đảm bảo rằng độ trễ của gói tin được xử lý không vượt quá 03 ms.

5.2. Thời gian phát hiện tấn công

Đối với các dạng tấn công tại Mục II, khoản 6, Anti-DDoS đảm bảo thời gian phát hiện tấn công tối đa là 03 phút từ lúc có tấn công DDoS xảy ra.

5.3. Băng thông chống tấn công

Anti-DDoS cho phép xử lý các cuộc tấn công DDoS băng thông tối thiểu 1Gbps/01 thiết bị.

5.4. Khả năng chặn lọc lưu lượng tấn công

a) Anti-DDoS đảm bảo khả năng phát hiện và chặn lọc lưu lượng tấn công tối thiểu 80%.

b) Anti-DDoS đảm bảo khả năng bảo vệ lưu lượng sạch tối thiểu 85%.

6. Yêu cầu về khả năng bảo vệ

Anti-DDoS đảm bảo dịch vụ của khách hàng vẫn hoạt động bình thường trước tối thiểu các loại tấn công DDoS sau bao gồm:

a) Tấn công làm tràn ngập băng thông: UDP reflection (DNS, NTP amplification, SSDP attack, Chargen attack), IP fragment, ICMP flood và các dạng tấn công tương tự;

b) Tấn công cạn kiệt tài nguyên qua giao thức TCP: SYN flood, ACK flood, RST flood, SYN-ACK flood và các dạng tấn công tương tự;

c) Tấn công sử dụng gói tin không hợp lệ: malformed, invalid packet;

d) Tấn công gửi gói tin/yêu cầu với tần suất cao, đột ngột;

đ) Tấn công qua phân tích hành vi người dùng: HTTP page flood, DNS flood, brute force;

e) Khả năng chặn lọc gói tin theo chính sách sử dụng ALC.

7. Yêu cầu về cảnh báo

7.1. Cấu hình cảnh báo

Anti-DDoS cho phép cấu hình cảnh báo cho người dùng bao gồm:

a) Cho phép cấu hình nội dung gửi cảnh báo qua một trong các cách thức sau: Email/SMS/OTT;

b) Cho phép cấu hình nhiều người nhận trong cùng một thời gian qua Email hay SMS;

c) Cho phép cấu hình chỉ gửi cảnh báo dựa trên các điều kiện mong muốn (ví dụ: mức độ tấn công, địa chỉ IP bị tấn công);

d) Cho phép cấu hình cảnh báo riêng biệt theo các nhóm địa chỉ IP bảo vệ khác nhau;

đ) Cho phép cấu hình các ngưỡng phát hiện cảnh báo tấn công theo từng nhóm địa chỉ IP bảo vệ khác nhau.

7.2. Cảnh báo theo thời gian thực

Anti-DDoS cho phép tự động cảnh báo tới người dùng theo thời gian thực đối với các loại sự kiện sau.

a) Cảnh báo khi có tấn công DDoS xảy ra;

b) Cảnh báo về tự động xử lý tấn công DDoS;

c) Cảnh báo khi tấn công DDoS kết thúc.

8. Yêu cầu về giám sát

Anti-DDoS cho phép giám sát và phân tích sự cố tấn công DDoS:

a) Cho phép giám sát thông tin các cuộc tấn công xảy ra theo thời gian thực và tìm kiếm trong các cuộc tấn công đã xảy ra;

b) Cho phép giám sát băng thông theo địa chỉ IP và dải mạng phục vụ phân tích tấn công;

c) Cho phép giám sát theo dõi hiệu quả chặn lọc thông qua lưu lượng băng thông trước và sau khi đi qua bộ lọc.

9. Yêu cầu về tự động hóa

Anti-DDoS cho phép quản lý bảo vệ tự động địa chỉ IP bị tấn công được cấu hình trên hệ thống:

a) Cho phép cấu hình kịch bản (điều kiện) tự động bảo vệ địa chỉ IP khi phát hiện được tấn công xảy ra;

b) Cho phép tự động tạo ra ACL ngăn chặn tấn công dựa trên đặc điểm tấn công phát hiện được;

c) Cho phép tự động bỏ bảo vệ, trả về điều kiện ban đầu khi phát hiện tấn công đã kết thúc;

d) Thông báo cho người dùng khi địa chỉ IP được tự động bảo vệ.