Bkav Anti-ddos

STT	Tính năng	Chi tiết	
1	Quản lý vận hành	Anti-DDoS cho phép quản lý vận hành đáp ứng các yêu cầu sau:	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;
			Cho phép thiết lập thời gian hệ thống thủ công hoặc được cập nhật tự động
			Cho phép thay đổi thời gian duy trì phiên kết nối;
			Cho phép đăng xuất tài khoản người dùng mà phiên kết nối còn hiệu lực.
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:	Hỗ trợ phương thức xác thực bằng tài khoản - mật khẩu
			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.
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:	Cho phép tạo mới theo thời gian muốn xuất báo cáo;
			Cho phép tải về báo cáo theo chu kỳ thời gian.
4	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.	
5	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.	
6	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.	
7	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.	
8	Log quản trị hệ thống	Anti-DDoS cho phép ghi log quản trị hệ thống về các loại sự kiện sau:	Thay đổi ACL của hệ thống cho từng địa chỉ IP;
			Thay đổi về route/rollback một địa chỉ IP ra khỏi hệ thống;
			Thông tin kết quả lệnh tương tác với bộ định tuyến trên mạng lưới để route/rollback hệ thống
		Anti-DDoS cho phép ghi log quản trị hệ thống có các trường thông tin sau:	Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây);
			Định danh của tác nhân thực hiện quản trị hệ thống (ví dụ: tài khoản người dùng, tên hệ thống,…)
			Định danh của đối tượng tác động (địa chỉ IP bị tác động);
			Thông tin chi tiết về các thay đổi cấu hình hệ thống bởi người quản trị (ví dụ: danh sách ACL bị thay đổi);
			Kết quả thực hiện việc thay đổi cấu hình hệ thống bởi người quản trị (thành công hoặc thất bại)
9	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.	
10	Quản lý log	Anti-DDoS cho phép quản lý log đáp ứng các yêu cầu sau:	Cho phép tìm kiếm log theo từ khóa theo thời gian và theo đối tượng;
			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.
11	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	
12	Thời gian phát hiện tấn	Anti-DDoS đảm bảo thời gian phát hiện tấn công tối đa là 03 phút từ lúc có tấn công DDoS xảy ra.	
13	Băng thông chống tấn công	Anti-DDoS cho phép xử lý các cuộc tấn công DDoS băng thông tối thiểu 1Gbps/01 thiết bị	
14	Khả năng chặn lọc lưu lượng tấn công	Anti DDoS đảm bảo khả năng phát hiện và chặn lọc lưu lượng tấn công tối thiểu 80%.	
		Anti DDoS đảm bảo khả năng bảo vệ lưu lượng sách tối thiểu 85%.	
15	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:	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;	
		Tấn công cạn kiệt tài nguyên giao thức TCP: SYN flood, ACK flood, RST flood, SYN-ACK flood và các dạng tấn công tương tự;	
		Tấn công sử dụng gói tin không hợp lệ: malformed, invalid packet;	
		Tấn công gửi gói tin/yêu cầu với tần suất cao, đột ngột;	
		Tấn công qua phân tích hành vi người dùng: HTTP page flood, DNS flood, brute force;	
		Khả năng chặn lọc gói tin theo chính sách sử dụng ALC	
16	Cấu hình cảnh báo	Anti-DDoS cho phép cấu hình cảnh báo cho người dùng bao gồm:	Cho phép cấu hình nội dung gửi cảnh báo qua một trong các cách thức sau: Email/SMS/OTT;
			Cho phép cấu hình nhiều người nhận trong cùng một thời gian qua Email hay SMS;
			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);
			Cho phép cấu hình cảnh báo riêng biệt theo các nhóm địa chỉ IP bảo vệ khác nhau;
			Cho phép cấu hình các ngưỡng phát hiện cảnh báo tấn công theo từng nhóm địa chỉ IP bảo vệ khác nhau.
17	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.	Cảnh báo khi có tấn công DDoS xảy ra;
			Cảnh báo về tự động xử lý tấn công DDoS;
			Cảnh báo khi tấn công DDoS kết thúc
18	Anti-DDoS cho phép giám sát và phân tích sự cố tấn công DDoS:	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;	
		Cho phép giám sát băng thông theo địa chỉ IP và dải mạng phục vụ phân tích tấn công;	
		Cho phép giám sát theo dõi hiệu quả chặn lọc thông qua lưu lượng băng thông trước và sau khi đi qua bộ lọc.	
19	Anti-DDoS cho phép quản lý bảo vệ tự động địa chỉ IP bị tấn công được cấu hình trên hệ thống:	Cho phép cấu hình kịch bản (điều kiện) tự động bảo vệ địa chỉ IP khi phát hiện được tấn công xảy ra;	
		Cho phép tự động tạo ra ACL ngăn chặn tấn công dựa trên đặc điểm tấn công phát hiện được;	
		Cho phép tự động bỏ bảo vệ trả về điều kiện ban đầu khi phát hiện tấn công đã kết thúc;	
		Thông báo cho người dùng khi địa chỉ IP được tự động bảo vệ.	

Trụ sở chính: Tòa nhà Bkav, Khu đô thị Yên Hòa, Cầu Giấy, Hà Nội
Điện thoại: (024) 3763 2552 So fax: (024) 3868 4755
Website: security.bkav.com Email: security@bkav.com
Bkav TP. HCM: So 67, Đường số 3, Khu dân cư City Land, P. 7, Q. Gò Vấp, TP HCM
Điện thoại: (028) 6296 6626 So fax: (028) 2253 6103