BKAV WAF

STT	Tính năng	Mô tả
1	Quản lý vận hành	Cho phép thiết lập, thay đổi, áp dụng và hoàn tác sự 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 luật bảo vệ;
		Cho phép thay đổi thời gian hệ thống;
		Cho phép thay đổi thời gian duy trì phiên kết nối;
		Cho phép thiết lập, thay đổi các tham số giới hạn đối với kết nối quản trị từ xa (ví dụ: giới hạn địa chỉ IP, giới hạn số phiên kết nối quản trị từ xa đồng thời,…);
		Cho phép đăng xuất tài khoản người dùng có phiên kết nối còn hiệu lực;
		Cho phép tìm kiếm dữ liệu log bằng từ khóa để xem lại;
		Cho phép xóa log;
		Cho phép xem thời gian hệ thống chạy tính từ lần khởi động gần nhất.
2	Quản trị từ xa	Sử dụng giao thức có mã hóa như TLS hoặc tương đương;
		Tự động đăng xuất tài khoản và hủy bỏ phiên kết nối quản trị từ xa khi hết thời gian duy trì phiên kết nối.
3	Quản lý xác thực và phân quyền	Hỗ trợ phương thức xác thực bằng tài khoản - mật khẩu, trong đó, quản trị viên có thể thiết lập và thay đổi được độ phức tạp của 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.
4	Quản lý báo cáo	Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo;
		Cho phép tạo báo cáo mới theo các mẫu báo cáo đã được định nghĩa trước;
		Cho phép áp dụng các quy tắc tìm kiếm thông tin, dữ liệu log để thêm, lọc, tinh chỉnh nội dung cho báo cáo;
		Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 02 trong các định dạng sau: WORD, EXCEL, PDF, HTML, XML;
		Cho phép tải về tệp tin báo cáo đã được xuất ra.
5	Quản lý tập luật bảo vệ	Thêm luật mới;
		Tinh chỉnh luật;
		Tìm kiếm luật;
		Xóa luật;
		Kích hoạt/vô hiệu hóa luật;
		Xuất tập luật ra tệp tin;
		Khôi phục tập luật từ tệp tin;
		Cập nhật tập luật được phát hành bởi nhà sản xuất.
6	Cập nhật tập luật bảo vệ	Cho phép tự động thông báo có bản cập nhật mới cho quản trị viên;
		Cho phép tải về trực tuyến và áp dụng thủ công bản cập nhật mới.
7	Bảo vệ cấu hình	Cấu hình hệ thống;
		Cấu hình quản trị từ xa;
		Cấu hình tài khoản xác thực và phân quyền người dùng;
		Cấu hình tập luật bảo vệ.
8	Bảo vệ dữ liệu log	Trong trường hợp WAF phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), WAF đảm bảo các loại cấu hình sau mà đang được áp dụng phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp:
9	Đồng bộ thời gian hệ thống	Trong trường hợp WAF phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), WAF đảm bảo thời gian hệ thống phải được đồng bộ tự động đến thời điểm hiện tại.
10	Khả năng chịu lỗi vận hành	Trong trường hợp WAF gặp lỗi trong quá trình thực thi tập luật bảo vệ mà không thể tự động khắc phục được, WAF 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.
11	Log quản trị hệ thống	WAF cho phép ghi log quản trị hệ thống về các loại sự kiện sau:
		Đăng nhập, đăng xuất tài khoản;
		Xác thực trước khi cho phép truy cập vào tài nguyên, sử dụng chức năng của hệ thống;
		Áp dụng, hoàn tác sự 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 luật bảo vệ;
		Kích hoạt lệnh khởi động lại, tắt hệ thống;
		Thay đổi thủ công thời gian hệ thống.
		WAF 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);
		Địa chỉ IP hoặc định danh của máy trạm;
		Định danh của tác nhân (ví dụ: tài khoản người dùng, tên hệ thống,…);
		Thông tin về hành vi thực hiện (ví dụ: đăng nhập, đăng xuất, thêm, sửa, xóa, cập nhật, hoàn tác,…);
		Kết quả thực hiện hành vi (thành công hoặc thất bại).
		Lý do giải trình đối với hành vi thất bại (ví dụ: không tìm thấy tài nguyên, không đủ quyền truy cập,…).
12	Log chức năng bảo vệ ứng dụng web	WAF cho phép ghi log chức năng bảo vệ ứng dụng web về các loại sự kiện sau:
		Truy cập vào tài nguyên của ứng dụng web được bảo vệ;
		Cảnh báo được sinh ra bởi việc thực thi tập luật bảo vệ.
		WAF cho phép ghi log chức năng bảo vệ ứng dụng web có các trường thông tin sau:
		Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây);
		Địa chỉ IP hoặc định danh của máy nguồn;
		Địa chỉ IP hoặc định danh của máy đích;
		Số hiệu cổng nguồn;
		Số hiệu cổng đích;
		Tên giao thức (HTTP hoặc HTTPS);
		Đường dẫn và danh sách tham số của URL;
		Phương thức truy vấn (ví dụ: GET, POST, HEAD,…);
		Mã trạng thái phản hồi (ví dụ: 200, 404,…);
		Cách thức xử lý của luật bảo vệ khi có cảnh báo được sinh ra (ví dụ: từ chối khởi tạo kết nối, hủy kết nối hiện hành, điều hướng kết nối đến máy chủ khác,…).
		Lý do giải trình đối với cách thức xử lý của luật bảo vệ.
13	Quản lý log	Cho phép thiết lập và cấu hình các cài đặt liên quan đến lưu trữ và hủy bỏ log (ví dụ: ngưỡng giới hạn dung lượng lưu trữ, khoảng thời gian lưu trữ,…).
		Cho phép tìm kiếm log theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có);
		Cho phép xuất dữ liệu log ra để phục vụ cho việc tích hợp các dữ liệu này vào SIEM hoặc giải pháp khác về quản lý, phân tích, điều tra log.
14	Kiểm soát thông tin trong log	WAF cho phép kiểm soát và che dấu các thông tin bí mật được thể hiện trong log như mật khẩu, mã xác thực một lần OTP và các loại giá trị bí mật khác dùng trong quá trình xác thực.
15	Đối với giao thức HTTP	Duy trì lên đến 30.000 kết nối trung bình mỗi giây;
		Duy trì lên đến 20.000 phiên kết nối liên tục đồng thời;
		Duy trì độ trễ trung bình gửi yêu cầu không quá 3 mili giây.
16	Đối với giao thức HTTPS	Duy trì lên đến 20.000 kết nối TLS/SSL trung bình mỗi giây;
		Duy trì lên đến 14.000 phiên kết nối TLS/SSL liên tục đồng thời;
		Duy trì độ trễ trung bình gửi yêu cầu không quá 5 mili giây.
17	Đối với việc áp dụng các sự thay đổi trong cấu hình tập luật bảo vệ	WAF cho phép áp dụng các sự thay đổi trong cấu hình tập luật bảo vệ mà không làm gián đoạn hoạt động của các ứng dụng web được bảo vệ quá 10 giây.
18	Phát hiện và ngăn chặn tấn công hệ thống	WAF có khả năng tự bảo vệ, ngăn chặn các dạng tấn công phổ biến sau vào giao diện ra bên ngoài của hệ thống, bao gồm tối thiểu các dạng sau:
		SQL Injection;
		OS Command Injection;
		XPath Injection;
		Remote File Inclusion (RFI);
		Local File Inclusion (LFI);
		Cross-Site Scripting (XSS);
		Cross-Site Request Forgery (CSRF).
19	Cập nhật bản vá hệ thống	WAF cho phép cập nhật bản vá để xử lý các điểm yếu, lỗ hổng bảo mật của hệ thống mà đã được công bố.
20	Phát hiện và ngăn chặn tấn công ứng dụng web được bảo vệ	WAF có khả năng ngăn chặn tối thiểu các dạng tấn công phổ biến sau vào các ứng dụng web được bảo vệ:
		SQL Injection;
		OS Command injection;
		XPath Injection;
		Brute-force;
		Remote File Inclusion (RFI);
		Local File Inclusion (LFI);
		Cross-Site Scripting (XSS);
		Cross-Site Request Forgery (CSRF).
21	Cơ chế thực thi bảo vệ	Cơ chế dựa trên phân tích tập luật bảo vệ;
		Cơ chế dựa trên phân tích thông tin về hành vi truy cập ứng dụng web;
		Cơ chế dựa trên phát hiện và sửa đổi thông tin có nội dung độc hại trên URL của gói tin yêu cầu gửi đến ứng dụng web.
22	Che giấu thông tin về ứng dụng web được bảo vệ	WAF cho phép che giấu các thông tin về hệ điều hành máy chủ, kiến trúc nền tảng web,… của ứng dụng web được bảo vệ.
23	Hỗ trợ giao thức TLS/SSL	Đối với các giao dịch của ứng dụng web có sử dụng giao thức HTTPS, WAF cho phép sử dụng các phiên bản giao thức có mã hóa TLS/SSL.
24	Tùy biến cấu hình tập luật bảo vệ theo đối tượng	Tùy biến cấu hình tập luật bảo vệ theo đối tượng
25	Thiết lập cấu hình giao thức	Cấu hình hỗ trợ giao thức ứng dụng web HTTP/HTTPS;
		Cấu hình phương pháp mã hóa/giải mã ký tự;
		Thiết lập các tham số của giao thức (ví dụ: giới hạn kích thước gói tin yêu cầu, giới hạn kích thước gói tin phản hồi, giới hạn độ dài phần tiêu đề của gói tin,…).

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 thoai: (028) 6296 6626 So fax: (028) 2253 6103