BKAV PAM

Mục lục

1.Tổng quan

- Bkav Privileged Access Management (Bkav PAM) là nhóm giải pháp giúp bảo mật, quản lý tập trung các tài khoản quản trị hệt hống, phiên truy cập đặc quyền một cách tự động trong việc kiểm soát truy cập tài nguyên, thiết lập, thay đổi chính sách và cấu hình trên hệ thống

2.Tính năng nổi bật và lợi ích của Hệ thống

- Quản lý và lưu trữ password tập trung, cho phép các tài khoản đăng nhập (hoặc truy cập trong trường hợp khẩn cấp) vào hệ thống mà không cần nhập các thông tin đăng nhập thực sự trên hệ thống đích.
- Có khả năng thay đổi mật khẩu ngẫu nhiên bằng cách lập lịch và bảo quản các mật khẩu đó trong vùng bảo mật. Có cơ chế đối soát nhằm xác định tình trạng password có bị thay đổi hay không hoặc phục hồi lại password trước đây.
- Người dùng tự động đăng nhập vào các phiên RDP và SSH, mà không cần nhập mật khẩu

- Thông báo theo thời gian thực dưới dạng mật khẩu được phát hành và hoạt động phiên đặc quyền được bắt đầu
- Hỗ trợ kiểm soát người dùng

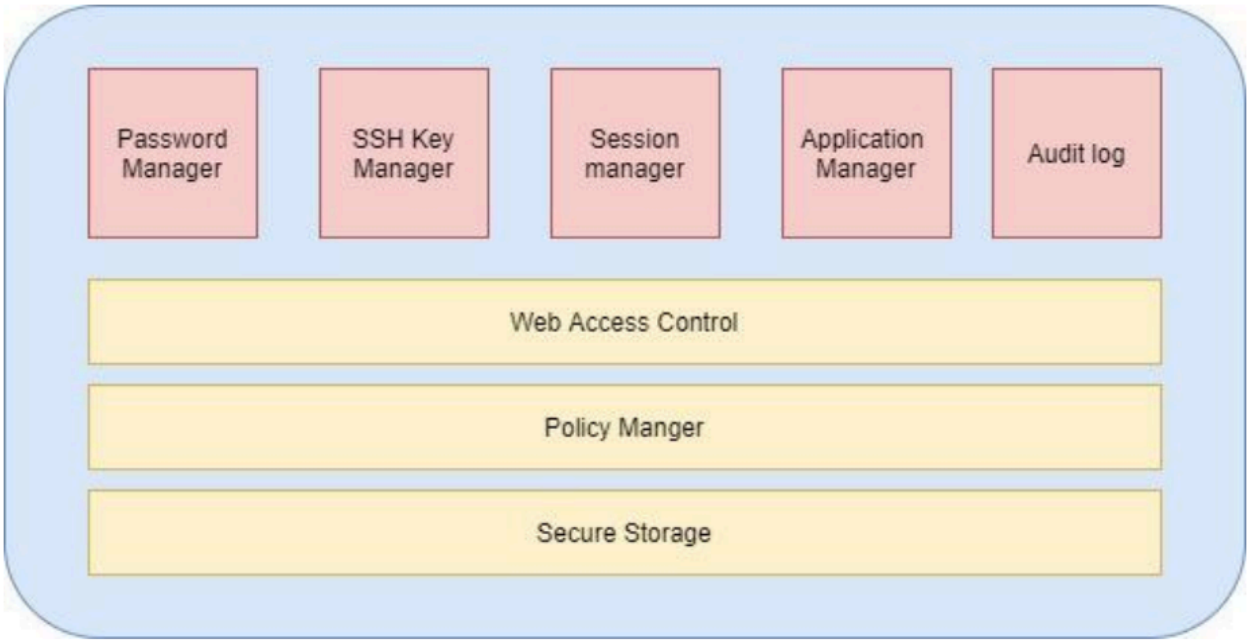
+ Can thiệp trực tiếp vào hành động của user (trực tiếp dừng hành động của user)

+ Kiểm soát và cho phép tìm kiếm các hành vi của người dùng tác động lên hệ thống thông qua hình ảnh được ghi lại. Từ đó, xác định rõ trách nhiệm của mỗi người dùng.

+ Cung cấp công cụ theo dõi, quản trị và báo cáo tổng thể về việc sử dụng của người dùng trong hệ thống (qua Dashboard và các báo cáo quản trị phân tích).

3.Sơ đồ hoạt động và cách hoạt động

3.1 Mô hình kiến trúc phần mềm

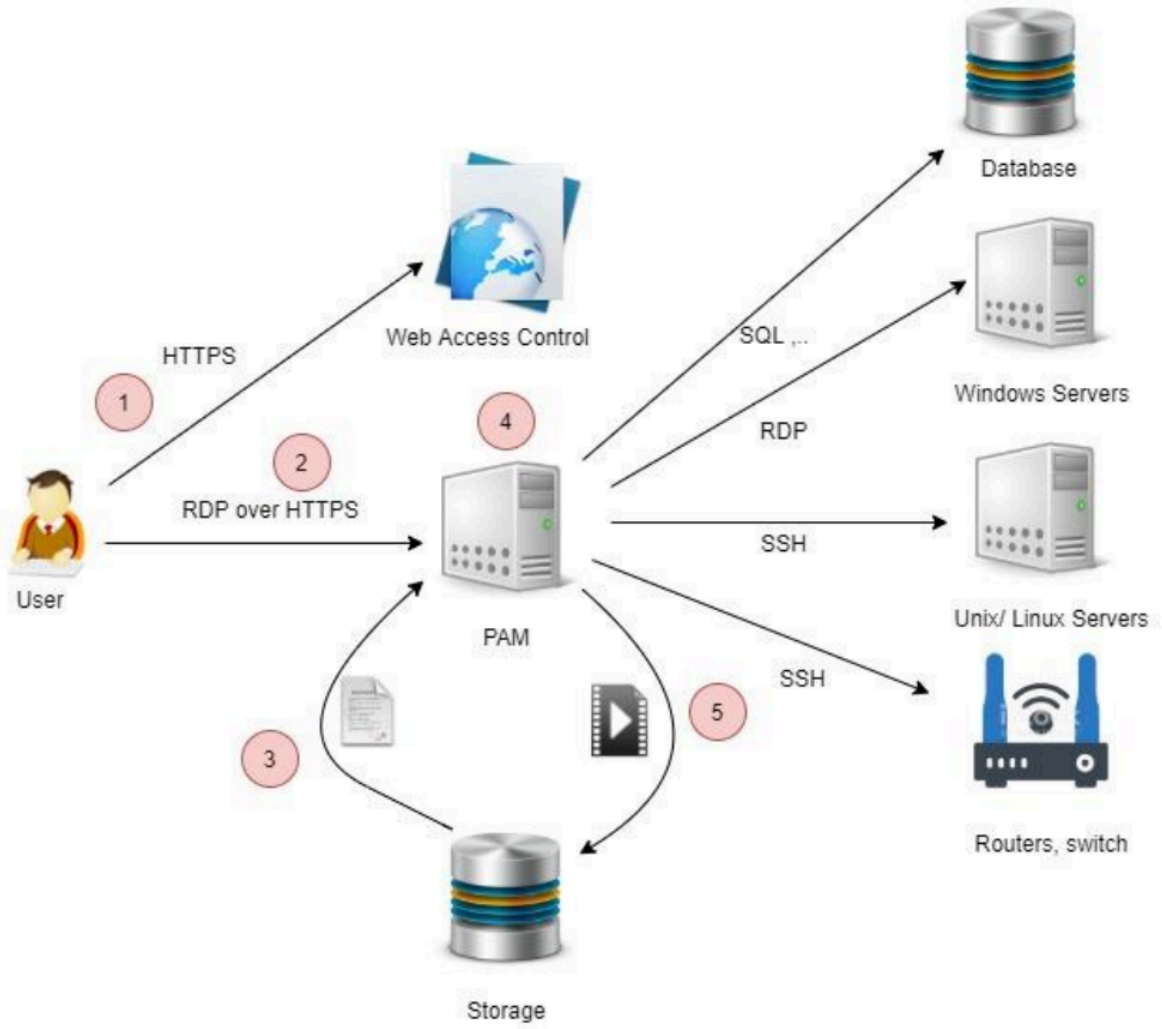


Các thành phần chính:

- Web Access Control là cổng thông tin cung cấp giao diện cho phép yêu cầu truy cập và mật khẩu đặc quyền vào các thiết bị.
- Session Manager ghi lại toàn bộ thao tác của người quản trị khi đăng nhập vào các thiết bị Bkav PAM quảnlý. Cho phép theo dõi trực tiếp thao tác và có thể ngắt các phiên làm việc.
- SSH Key Manager có chức năng lưu trữ quản lý tập trung và bảo mật cao các SSH Key trong Secure Storage. Tự động phân phối khóa trong quá trình sử dụng

- Password Manager có chức năng quản lý người mật khẩu, thay đổi mật khẩu định kỳ, phát hiện mật khẩu yếu
- Application Manager cung cấp việc xác thực ứng dụng trước khi cung cấp mật khẩu để sử dụng
- Policy Manager cung cấp việc cấu hình, quy trình quản lý truy cập, quản lý mật khẩu, quản lý phiên và kiểm soát việc ghi log trong Secure Storage

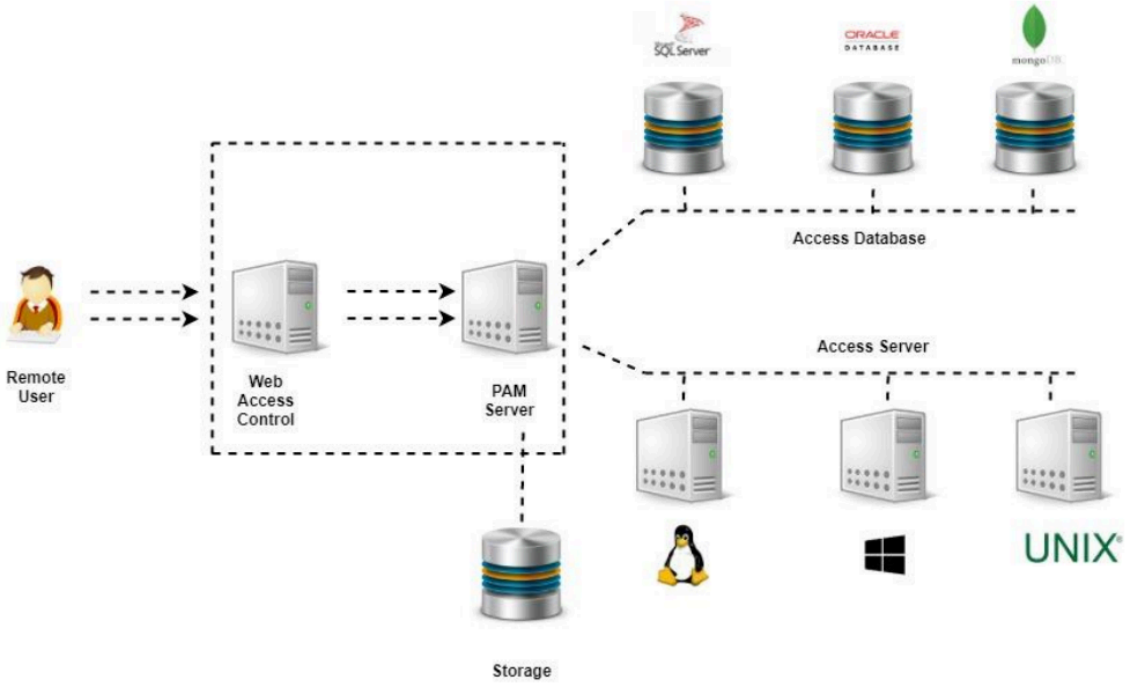
3.2 Sơ đồ Quy trình nghiệp vụ



- Khi sử dụng Bkav PAM, các quản trị viên thông qua giao diện ứng dụng web được cài đặt trên máy chủ Web Access Control để kết nối trực tiếp đến hệ thống đích, thông qua các giao thức hoặc tool khi kết nối trực tiếp.

- Quy trình thực hiện cho quản trị viên:
  - Truy cập hệ thống Bkav PAM qua giao diện Web Access Control
  - Chọn hệ thống để kết nối
  - Bkav PAM gửi cho quản trị viên IT file RDP hoặc SSH key
  - Mở file để kết nối (quản trị viên truy cập vào thiết bị mà không hề biết mật khẩu)
  - Mọi thao tác của quản trị viên được ghi lại và lưu trong Secure Storage

3.3 Mô hình kết nối/tích hợp với HT khác



Diễn giải:

PAM đóng vai trò quản lý các mật khẩu và phiên truy cập đặc quyền tự đông, cung cấp khả năng truy cập bảo mật và ghi lại hành vi của bất kỳ tài khoản nào - từ quản trị viên đến các tài khoản cá nhân, tài khoản database, ứng dụng. Bkav PAM cung cấp nhiều lựa chọn triển khai và hỗ trợ các nền tảng khác nhau.

4.Chi tiết tính năng

STT	Tên Tính năng	Mô tả
1	Chức năng đăng nhập	Dùng để đăng nhập vào hệ thống truy cập đặc quyền PAM
2	Quản lý danh mục tài nguyên	QL danh mục tài nguyên giúp cho Admin kiểm soát các tài nguyên mà hệ thống quản lý, thêm mới chỉnh sửa cấp quyền cho các user truy cập vào tài nguyên
3	Quản lý Resource role	Resource role giúp quản lý các quyền của tài nguyên có trên hệ thống.
4	Quản lý Tài khoản	Giúp quản lý các tài khoản truy cập hệ thống
5	Quản lý quyền truy cập của tài khoản	Thực hiện các chức năng liên quan đến cấp quyền truy cập tài khoản(tài khoản sẽ có quyền truy cập vào tài nguyên nào
6	Quản lý trạng thái tài nguyên	xem thông tin trạng thái của các tài nguyên đã được cấp quyền cho các tài khoản
7	Quản lý Log	Hệ thống sẽ theo dõi các phiên kể từ khi phiên diễn ra đến khi kết thúc phiên. Lưu lại thông tin liên quan đến các phiên
8	Quản lý cấu hình đăng nhập	cài đặt các chức năng liên quan đến đăng nhập
9	Quản lý cấu hình truy cập TN	Chỉnh sửa các cấu hình liên quan đến tài nguyên: số lượng truy cập tối đa, 1 tài nguyên có tối đa số phiên truy cập trong 1 thời điểm, bao nhiêu tài nguyên được phân quyền cho 1 tài khoản, một tài khoản được kết nối với bao nhiêu tài nguyên trong một thời điểm.

5. Yêu cầu phần cứng

	CPU	Ram	Disk
	4-8 CPU cores	8-16GB RAM	600GB