

GIẢI PHÁP ĐỀ XUẤT : QUẢN LÝ TRUY CẬP ĐẶC QUYỀN



MỤC LỤC

| | |
|--|-----------|
| 1. HIỆN TRẠNG QUẢN TRỊ HỆ THỐNG THÔNG TIN. | 4 |
| 1.1. Những nguy cơ tiềm ẩn bị tấn công từ ngay bên trong hệ thống mạng. | 4 |
| 1.2. Xu hướng bị tấn công từ bên trong diễn ra như thế nào trong 12 tháng qua? | 6 |
| 1.3. Tài khoản đặc quyền | 8 |
| 1.4. Những khó khăn trong quản lý tài khoản đặc quyền | 11 |
| 1.5. Các rủi ro và đe dọa từ tài khoản đặc quyền..... | 12 |
| 2. TỔNG QUAN VỀ GIẢI PHÁP QUẢN TRỊ ĐẶC QUYỀN (PRIVILEGED ACCESS MANAGEMENT – PAM) | 14 |
| 2.1. Giải pháp PAM là gì | 15 |
| 2.1.1 Lợi ích của giải pháp PAM | 16 |
| 2.1.2 Các tính năng của PAM | 16 |
| 2.2. Giải pháp PAM hoạt động như thế nào. | 17 |
| 2.3. PAM GIẢI QUYẾT VẤN ĐỀ GÌ CHO HẠ TẦNG..... | 19 |
| 3. ĐỊNH HƯỚNG LỰA CHỌN GIẢI PHÁP | 20 |
| 3.1. ĐỊNH HƯỚNG LỰA CHỌN GIẢI PHÁP | 20 |
| 3.2. GIẢI PHÁP ĐỀ XUẤT | 20 |
| 3.2.3 Thương hiệu và uy tín – là giải pháp hàng đầu thế giới | 20 |
| 3.2.4 Giới thiệu về WALLIX | 21 |
| 3.2.5 Giải pháp Wallix Bastion | 22 |
| 3.3. Các ưu điểm của giải pháp Wallix Bastion..... | 25 |
| 3.4. Bảo mật hệ thống | 27 |
| 3.5. Giải pháp đề xuất | 29 |
| 4. MÔ HÌNH TRIỂN KHAI ĐỀ XUẤT | 30 |
| 4.1. Mục tiêu của triển khai PAM | 30 |
| 4.1. Mô hình triển khai..... | 30 |
| 4.2. Quy trình xử lý lưu lượng | 31 |
| 4.3. Phương án triển khai mở rộng | 31 |

| | |
|--|-----------|
| 5. TÍNH NĂNG VÀ LỢI ÍCH CỦA GIẢI PHÁP | 33 |
| 5.1. Quản lý truy cập người dùng..... | 33 |
| 5.2. Cơ chế xác thực mạnh mẽ | 34 |
| 5.3. Quản lý tài khoản người dùng đơn giản, thuận tiện. | 35 |
| 5.4. Quản lý “kho” lưu trữ thông tin tài khoản thực, thông tin thiết bị thuận tiện | 38 |
| 5.5. <i>Chế độ SSO mode</i> | 38 |
| 5.6. Traceability – tính năng truy vết | 38 |
| 5.7. Vai trò của mô đun Session Management..... | 39 |
| 5.7.1 Kiểm soát, giám sát và gửi cảnh báo theo thời gian thực | 40 |
| 5.7.2 Hỗ trợ kiểm soát truy cập đối với các giao thức RDP và SSH từ máy người dùng | 42 |
| 5.7.3 Tính năng Session Sharing | 50 |
| 5.7.4 Hỗ trợ quy trình xác nhận (Workflow Approval) | 51 |
| 5.8. Vai trò của mô đun Password Manager | 53 |
| 5.8.1 Quản lý xác thực tập trung với tính năng check in/ check out | 53 |
| 5.8.2 Tính năng tự động đổi mật khẩu | 54 |
| 5.9. Mô đun Access Manager (WAM) | 56 |
| 5.10. Tích hợp hoàn hảo với các hệ thống SIEM, IDS, và SAOR | 58 |
| 5.11. Báo cáo | 59 |
| 5.12. Hỗ trợ REST API..... | 60 |
| 5.13. Tích hợp giải pháp Anti-virus, DLP | 60 |
| 5.14. Mô đun BestSafe..... | 61 |
| 5.14.3 Cách thức hoạt động của BestSafe | 62 |
| 5.14.4 Tính năng của BestSafe | 62 |

1. HIỆN TRẠNG QUẢN TRỊ HỆ THÔNG THÔNG TIN.

Giới thiệu chung về [Client]

Với vai trò quan trọng như trên, [Client] là đơn vị đi đầu trong [ClientGroup] trong việc **Bảo Mật Toàn Diện** hạ tầng CNTT có quy mô lớn với số lượng thiết bị CNTT đa dạng cùng với nhiều ứng dụng khác nhau được sử dụng trong công tác chuyên môn.

1.1. Những nguy cơ tiềm ẩn bị tấn công từ ngay bên trong hệ thống mạng.

Hiện nay, cũng như nhiều tổ chức khác, [Client] đang phải đối mặt với thực tế là: những cuộc tấn công mạng gây ra thiệt hại lớn nhất không phải đến từ những mã độc hay những cuộc tấn công khởi phát từ bên ngoài, mà nó nằm **ngay bên trong hệ thống mạng** của cơ quan hay doanh nghiệp – Nguyên nhân đến từ sự thiếu cẩn trọng và khoa học trong việc giám sát, kiểm toán và quản lý quyền truy cập của những nhân viên quản trị mạng hay những đối tác bên ngoài vào trong hệ thống.

Một mối đe dọa trong nội bộ được định nghĩa là mối đe dọa rằng một nhân viên hoặc nhà thầu sẽ sử dụng quyền truy cập được ủy quyền của mình, một cách khéo léo hoặc vô tình, để làm tổn hại đến an ninh của hệ thống.

Khi các tổ chức thực hiện các biện pháp an ninh mạng và vật lý ngày càng tinh vi để bảo vệ tài sản của họ khỏi các mối đe dọa bên ngoài, việc tuyển dụng nhân viên bên trong hay cài người vào trong hệ thống trở thành một lựa chọn hấp dẫn, dễ dàng hơn nhằm cố gắng giành quyền truy cập trái phép vào hệ thống.

Những mối nguy tiềm ẩn bên trong từ việc lơ là của đội ngũ quản trị mạng

Các mối đe dọa trong nội bộ không phải lúc nào cũng được tạo ra với mục đích phá hoại. Trên thực tế, nhiều mối đe dọa trong nội bộ tồn tại do những sự cố ngoài ý muốn hoặc vô tình.

Nhiều tấn công nội gián tình cờ xuất phát từ sự sơ suất của nhân viên quản trị và nhà thầu. Do các sơ xuất này, hệ thống CNTT bao gồm Cơ sở dữ liệu (CSDL), máy chủ, các ứng dụng hệ thống, thiết bị hạ tầng, đặc biệt khi xu hướng sử dụng hạ tầng máy bàn ảo hóa (Virtual Desktop Infrastructure- VDI), v.v luôn hứng chịu nguy cơ cao bị tấn công.

Nhiều tấn công nội gián tình cờ xuất phát từ sự sơ suất của nhân viên quản trị và nhà thầu. Do các sơ xuất này, hệ thống CNTT bao gồm Cơ sở dữ liệu (CSDL), máy chủ, các ứng dụng hệ thống, thiết bị hạ tầng, đặc biệt khi xu hướng sử dụng hạ tầng máy bàn ảo hóa (Virtual Desktop Infrastructure- VDI), v.v luôn hứng chịu nguy cơ cao bị tấn công.

Trong thực tế quản trị hệ thống, nhiều chính sách bảo mật bị bỏ qua. Trong đó, các lỗi thường gặp nhất là mật khẩu tương tự cho nhiều tài khoản, chia sẻ mật khẩu bất cẩn, sử dụng WiFi không bảo mật và giữ các thiết bị không có mật khẩu, và không có chính sách thay đổi mật khẩu định kỳ cũng như đặt mật khẩu không đạt chuẩn.

Các nghiên cứu về các mối đe dọa trong nội bộ cũng cho thấy nguy cơ tấn công nội bộ đặc biệt tăng cao trong môi trường có rất nhiều người dùng có quyền truy cập không hạn chế và quá mức như thực trạng hiện nay tại các trung tâm dữ liệu của C86. Ngoài ra, việc lưu trữ phi tập trung dữ liệu nhạy cảm trên nhiều thiết bị, cũng như không kiểm soát các dữ liệu nhạy cảm và bỏ qua việc đào tạo nâng cao ý thức của các nhân viên quản trị cũng là những yếu tố quan trọng làm tăng cao các mối đe dọa nội bộ.



Một nghiên cứu năm 2016 đã cho thấy trong tổng số 874 sự cố, 568 là do sự thiếu hiểu biết của nhân viên quản trị và nhà thầu, 85 sự cố gây ra bởi người ngoài thông qua truy cập thông tin xác thực và 191 gây ra bởi những kẻ xâm nhập và tin tặc với ý đồ phá hoại.

Theo 1 báo cáo của quốc tế mới nhất về các mối đe dọa đến từ việc khảo sát những Giám đốc IT hay trưởng phòng IT của các tổ chức lớn cho thấy Các mối đe dọa đến từ trong nội bộ vẫn là những vấn đề cấp bách hàng đầu, lý do là: **64% nhân viên quản trị hệ thống mạng thừa nhận rằng họ đã vi phạm quyền truy cập** do đã sử dụng không đúng chức năng quyền truy cập vào mạng hoặc lạm dụng quyền truy cập khi không có ai giám sát quản lý.

58% trong số này thừa nhận đã **chia sẻ tài khoản quản trị trái phép**, **56%** thường xuyên **không thoát khỏi tài khoản quản trị** sau khi hoàn thành công việc.



Tác động của mối phân tích về nguy cơ tấn công từ nội bộ

Một Báo cáo phân tích về nguy cơ tấn công từ nội bộ 2017 cho thấy cùng với việc mất dữ liệu, các tấn công này còn gây ra thiệt hại lớn về tài chính. Theo báo cáo này, 53% các tổ chức được khảo sát tuyên bố rằng họ phải đầu tư chi phí khắc phục khoảng 100.000 đô la trở lên, trong đó có tới 12% tổ chức được hỏi ước tính chi phí này là hơn 1 triệu đô la.

Một báo cáo Phân tích về nguy cơ tấn công từ nội bộ năm 2018 cho thấy 66% các tổ chức xem trọng việc ngăn chặn các nguy cơ tấn công nội gián độc hại hoặc vô tình nhiều khả năng hơn các cuộc tấn công bên ngoài. Phần lớn các tổ chức đánh giá mối phân tích về nguy cơ tấn công từ nội bộ gây thiệt hại nhiều hơn so với các cuộc tấn công từ bên ngoài. Nhưng câu hỏi là tại sao các tổ chức không thể ngăn chặn các mối đe dọa này ngay cả sau khi thừa nhận?

Dưới đây là một số lý do có thể xảy ra;

- Các mối đe dọa trong nội bộ là rất khó để phát hiện, vì hầu hết chúng là vô ý và đột ngột. Có thể có nhiều năm mà mối đe dọa trong nội bộ tồn tại mà có thể không bị phát hiện. Một số nghiên cứu cho thấy hầu hết các cuộc tấn công nội bộ được phát hiện trong vòng vài phút hoặc vài ngày. Nghiên cứu khác chỉ ra rằng phải mất từ vài tháng đến vài năm để phát hiện ra một vi phạm như vậy. Trung bình mất 197 ngày để phát hiện và **69 ngày để ngăn chặn nó**.
- Phân biệt thê nào là mối đe dọa trong công việc thường xuyên cũng là một nhiệm vụ khó khăn. Một nhân viên làm việc với dữ liệu nhạy cảm hoặc thông tin đăng nhập có thể thực hiện nhiệm vụ thường xuyên của mình. Rất khó để theo dõi toàn bộ quá trình làm việc nếu không có công cụ phù hợp.
- Người trong cuộc hoặc nhân viên quản trị có cơ hội dễ dàng che dấu hành động của họ. Nếu muốn, người có ý đồ hoan toàn có thể dễ dàng xóa các dấu hiệu của lỗ hổng trước khi bắt cứ ai nhìn thấy nó.
- Cuối cùng, nếu quản lý phát hiện mối đe dọa trong nội bộ, nhân viên gây ra mối đe dọa có thể thoát khỏi việc phán xét bằng cách tuyên bố hành động của mình là một sai lầm.

Do những vấn đề như trên, nhân viên quản trị cũng như những người có liên quan đến quản trị hệ thống tự phát hình thành các hành vi bất cẩn và không quan tâm đến hậu quả

Kiểm soát và phát hiện rủi ro

Có nhiều biện pháp thông qua đó chúng ta có thể phát hiện và kiểm soát các mối đe dọa trong nội bộ trong tổ chức của mình. Vì dụ như mã hóa dữ liệu, ngăn ngừa mất dữ liệu, quản lý truy cập và nhận dạng, bảo mật thiết bị đầu cuối và di động và bảo mật truy cập đám mây; Biện pháp dùng hệ thống Log, quản lý sự kiện thông tin bảo mật (SIEM); đặc biệt là biện pháp **Hạn chế truy cập của các nhân viên quản trị và giáo dục, đào tạo nhân viên quản trị về an ninh thông tin**

Hạn chế quyền truy cập là chìa khóa quan trọng để giảm thiểu mọi mối đe dọa trên mạng. Cung cấp ít đặc quyền hơn sẽ hạn chế cơ hội khai thác độc hại do có ít tài khoản hơn và ít người dùng đặc quyền hơn. Do đó, chúng ta có thể làm giảm nguy cơ sai lầm vô tình hay cố ý Ngoài ra, chúng ta nên theo dõi và kiểm soát truy cập thông qua các máy chủ tập trung. Một số biện pháp bổ trợ giúp việc hạn chế truy cập hiệu quả hơn là nên được áp dụng như việc sử dụng mật khẩu mạnh và duy nhất, cấm chia sẻ mật khẩu và sử dụng xác thực hai yếu tố.

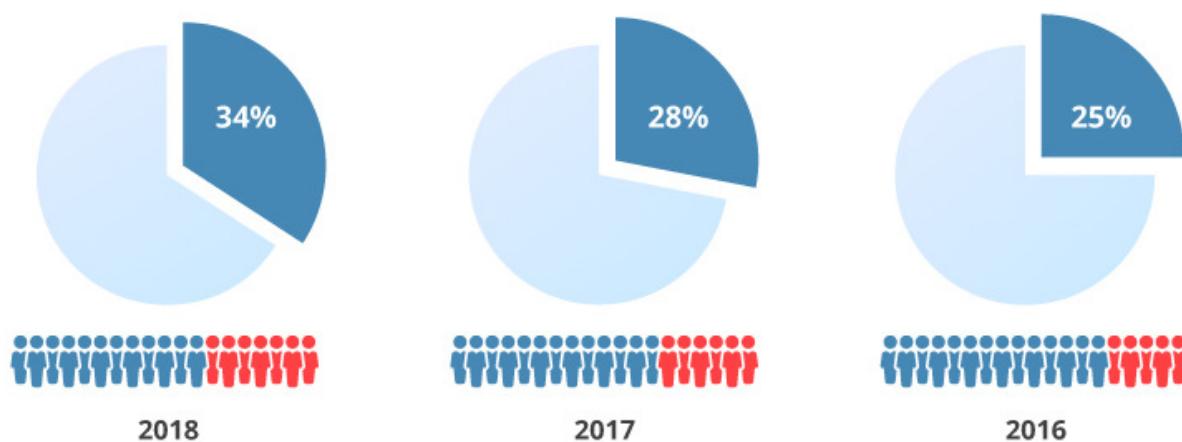
Giáo dục và đào tạo nhân viên

Yếu tố cuối cùng nhưng quan trọng nhất để giảm thiểu các mối đe dọa trong nội bộ là đào tạo nhân viên của bạn về các mối đe dọa an ninh mạng và các kênh mà qua đó lỗ hổng có thể được đưa vào.

Giáo dục đội ngũ tổ chức của bạn để thực hành bảo mật là một bước cần thiết. Nếu những người trong cuộc nhận thức được trách nhiệm của họ và hành vi thiếu hiểu biết có thể gây tổn hại cho tổ chức, họ sẽ tự chăm sóc và nhận thức.

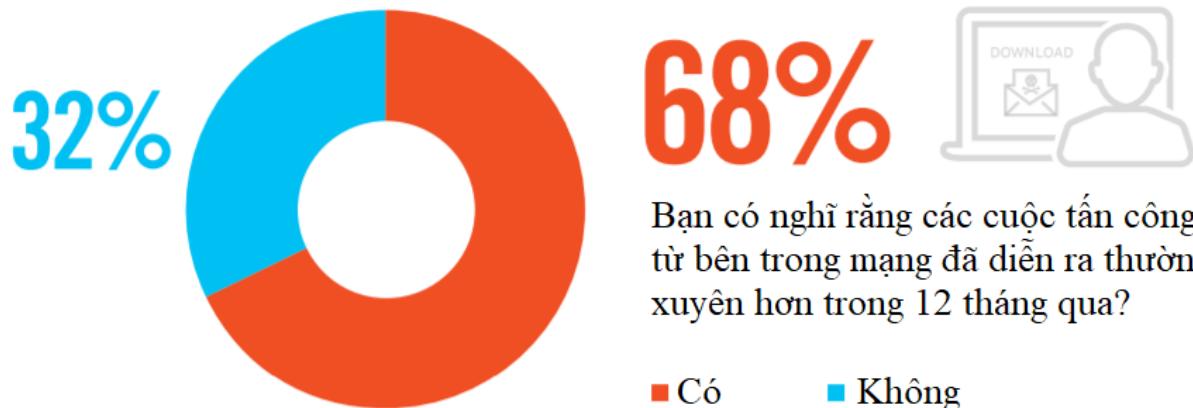
1.2. Xu hướng bị tấn công từ bên trong diễn ra như thế nào trong 12 tháng qua?

Năm 2019 đã chứng kiến nhiều vi phạm an toàn thông tin nghiêm trọng xuất phát từ nội bộ như (Marriott, Tesla) và đắt nhất (Ngân hàng Quốc gia Punjab, Ngân hàng Suntrust); chứng tỏ các nguy cơ tấn công từ nội bộ vẫn là một trong những mối đe dọa chính đối với an ninh mạng của các tổ chức.



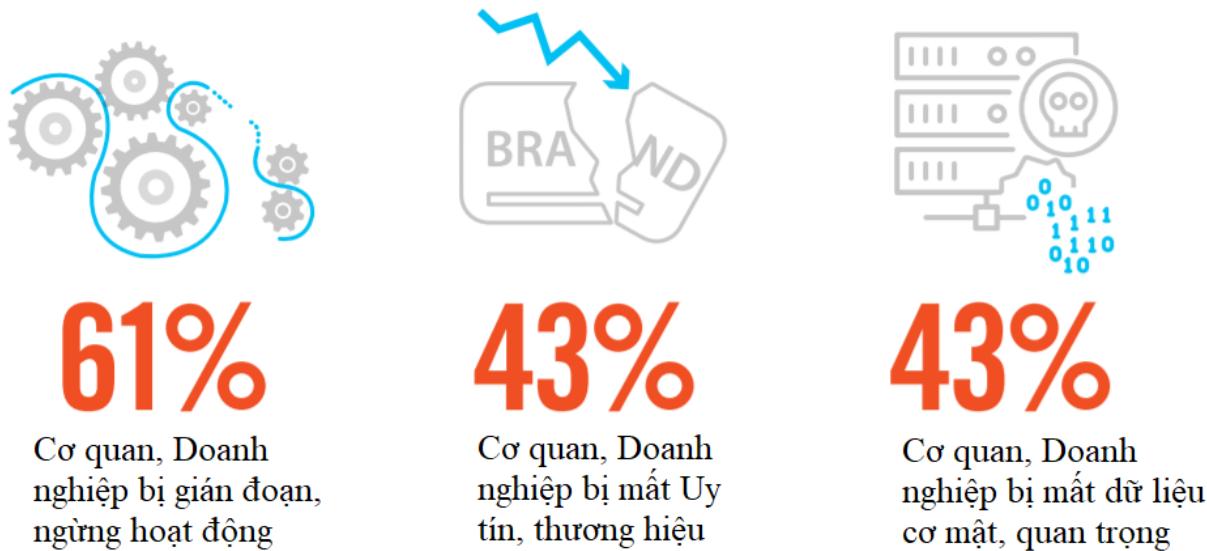
* Data provided by the 2017–2019 Verizon Data Breach Investigations reports

Đa số các cơ quan, đơn vị, doanh nghiệp được khảo sát cho thấy xu hướng bị tấn công từ bên trong ngày càng gia tăng trong 12 tháng qua. **68%** trong số họ nhận thấy điều này, và thực tế 67% đã bị 1 hoặc nhiều cuộc tấn công xuất phát từ trong mạng suốt 12 tháng qua.



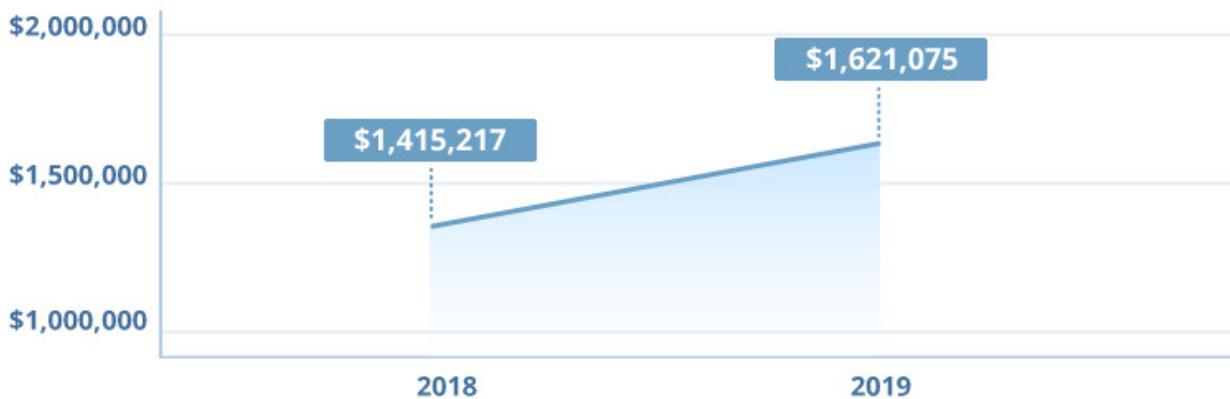
Những tổn thất mà các cuộc tấn công mạng xuất phát từ mạng nội bộ gây ra là gì?

Các cuộc tấn công xuất phát từ bên trong mạng đã gây ảnh hưởng nghiêm trọng đến hoạt động của các cơ quan đơn vị, nó khiến cho 61 % cơ quan bị gián đoạn hoặc bị tê liệt hoạt động, 43% bị mất uy tín và 43% cơ quan, doanh nghiệp bị mất những dữ liệu quan trọng.



Số liệu cho thấy ngày càng nhiều các tổ chức đã bị ảnh hưởng và chịu thiệt hại nặng từ các nguy cơ tấn công xuất phát hoặc liên quan đến nhân viên quản trị nội bộ.

Chi phí an ninh cho việc khắc phục khi hứng chịu các tấn công này ngày càng tiếp tục tăng cao



* Data provided by Accenture & Ponemon's 2019 Cost of Cybercrime Study

Đồng thời, các tác nhân, mô hình và cách tiếp cận bảo vệ nội bộ chính đang thay đổi. Thực tế đáng buồn là chúng ta buộc phải đầu tư nhiều hơn nữa cho an ninh mạng nếu muốn tiếp tục duy trì cũng như tăng cường mức độ bảo mật cho hệ thống. Nhiều quốc gia đã ra các bộ luật an ninh mạng. Thực tế cũng đã chứng minh, việc không tuân thủ sẽ khiến chúng ta trả giá đắt hơn theo thời gian bao gồm chi phí khắc phục hậu quả, chi phí phạt do không tuân thủ các bộ luật an ninh mạng cũng như chi phí trang bị, áp dụng các hệ thống an ninh mạng nhằm khắc phục lỗ hổng. Hệ thống càng ngày càng phức tạp, đồng nghĩa chi phí và thời gian cần cho việc triển khai, độ phức tạp và rủi ro khi triển khai các giải pháp bảo mật càng trễ sẽ càng làm phát sinh thêm chi phí.

Điều quan trọng là chọn không phải là giải pháp phổ biến nhất trên thị trường mà là giải pháp phù hợp với nhu cầu của công ty bạn một cách hoàn hảo.

1.3. Tài khoản đặc quyền

Chúng ta cần hiểu được tài khoản đặc quyền là gì?

Tài khoản đặc quyền là tài khoản có quyền truy cập cấp cao hơn so với những tài khoản khác trong cơ quan, doanh nghiệp. Tài khoản đặc quyền có thể được gọi là tài khoản siêu người dùng (SuperUser), chủ yếu được sử dụng để quản trị bởi các nhân viên CNTT chuyên ngành và cung cấp sức mạnh hầu như không bị hạn chế để thực hiện các lệnh và thực hiện thay đổi hệ thống. Các tài khoản Superuser thường được biết đến với tên gọi Root trong hệ điều hành Unix / Linux và quản trị viên mạng (Administrator/Superuser) trong các hệ thống Windows.

Đặc quyền tài khoản Superuser có thể cung cấp quyền truy cập không hạn chế vào các tệp, thư mục và tài nguyên với các đặc quyền đọc / ghi / thực thi đầy đủ và khả năng hiển thị các thay đổi hệ thống trên mạng, như tạo hoặc cài đặt tệp hoặc phần mềm, sửa đổi tệp và cài đặt và xóa người dùng và dữ liệu. Superusers thậm chí có thể cắp và thu hồi bất kỳ quyền cho người dùng khác. Nếu sử dụng sai, do lỗi (chẳng hạn như vô tình xóa một tệp quan trọng hoặc nhập sai lệnh mạnh mẽ) hoặc với mục đích xấu, các tài khoản đặc quyền cao này có thể dễ dàng gây ra thiệt hại thảm khốc trên toàn hệ thống hoặc thậm chí toàn bộ doanh nghiệp.

Trong các hệ thống Windows, mỗi máy tính Windows có ít nhất một tài khoản quản trị viên. Tài khoản Administrator cho phép người dùng thực hiện các hoạt động như cài đặt phần mềm và thay đổi cấu hình và cài đặt cục bộ.

Người dùng với tài khoản đặc quyền truy cập ưu tiên này có thể ghi đè hoặc bỏ qua, một số hạn chế bảo mật nhất định và có thể bao gồm các quyền để thực hiện các hành động như tắt hệ thống, tải trình điều khiển thiết bị, định cấu hình mạng hoặc hệ thống, cung cấp và định cấu hình tài khoản và các trường hợp đám mây, v.v.

Tội phạm mạng nhắm mục tiêu đến các tài khoản đặc quyền vì nó có thể đầy nhanh quá trình truy cập vào các dữ liệu có giá trị của cơ quan hay doanh nghiệp. Với những đặc quyền có được qua các tài khoản quản trị, tin tức hay các mã độc cơ bản đã trở thành 1 phần quan trọng trong hệ thống mạng nội bộ. Đó là 1 thực trạng đáng báo động, đặc biệt với những tài khoản có quyền truy cập vào hệ thống ở cấp độ cao nhất. Hơn thế nữa hacker có thể dễ dàng xóa các dấu vết của mình để tránh bị phát hiện trong khi chúng đi qua môi trường CNTT bị xâm phạm.

Chúng ta biết rằng, con đường tấn công từ của các tin tặc theo một phương thức “chuỗi tấn công”. Ban đầu tin tặc khai thác những lỗ hổng trong mạng và những tài khoản quản trị có đặc quyền. Sau đó chúng xuất hiện thường xuyên hơn và khảo sát môi trường CNTT của cơ quan đó, rồi tìm kiếm thêm những thông tin bổ sung để nâng cao đặc quyền truy cập vào hệ thống, cũng như những dữ liệu quan trọng.

Những rủi ro đến từ quyền truy cập quản trị của các đối tác, nhà thầu, nhà cung cấp dịch vụ

Đa số các phòng ban CNTT có đủ thẩm quyền để quản trị và cấp quyền quản trị cho hệ thống. Vì vậy thông thường họ sẽ kiểm luôn công việc cấp quyền truy cập cho các đối tác, nhà cung cấp, các nhà thầu truy cập quản trị hệ thống trong mỗi dự án. Theo khảo sát của các tổ chức lớn, trung bình mỗi tuần có 182 các đối tác truy cập vào hệ thống của họ, với **58% trong số đó nhận định họ không thể kiểm soát việc truy cập của các đối tác này**.

Về lý tưởng, các tổ chức muốn triển khai mở rộng môi trường bảo mật từ cơ quan họ tới những đối tác cung cấp dịch vụ, tuy nhiên, đa số các tổ chức được khảo sát thực tế không thể kiểm soát an ninh các truy cập đặc quyền của các đối tác. Kết quả cho thấy chỉ có 29% biết được có bao nhiêu đối tác truy cập vào hệ thống của họ, và chỉ có 31% có thể tự tin trả lời có bao nhiêu tài khoản quản trị đã cấp cho đối tác để truy cập.



Khảo sát cho thấy hầu hết các tổ chức tiếp tục cấp quá nhiều đặc quyền trong khi đó không ưu tiên triển khai giải pháp PAM và không thực hiện nó một cách hiệu quả. PAM cần được xem là 1 trong những yếu tố quan trọng hỗ trợ cho quá trình chuyển đổi số.





1.4. Những khó khăn trong quản lý tài khoản đặc quyền .

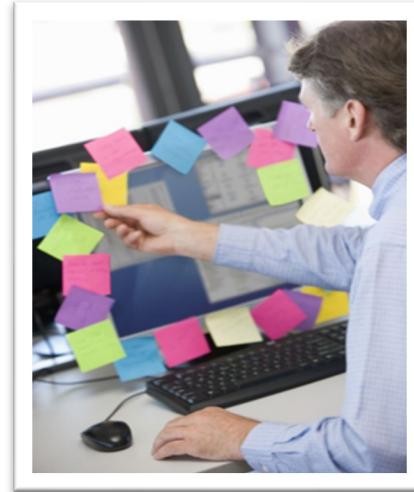
Với số lượng thiết bị đa dạng như hiện nay, việc quản trị hệ thống CNTT của [Client] theo 1 cách khoa học, loại bỏ những lỗ hổng bảo mật ngay từ bên trong hệ thống CNTT đang là 1 thách thức lớn giành cho đội ngũ quản trị hạ tầng CNTT. Dưới đây là những vấn đề cụ thể:

1. Quản lý, ghi nhớ số lượng tài khoản và phân quyền người dùng đúng với chức trách của họ.

Với số lượng thiết bị và các ứng dụng chuyên môn ngày càng gia tăng như hiện nay, việc lưu trữ các tài khoản quản trị đảm bảo đúng tiêu chuẩn bảo mật chung và của từng ứng dụng, thiết bị, không bị chồng chéo là một vấn đề khiên các cán bộ nhân viên IT đau đầu.

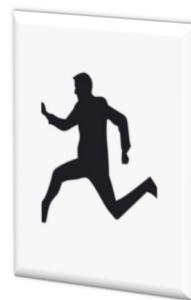
Với mỗi bộ phân riêng cần có 1 tài khoản có đặc quyền khác nhau không phải mọi người đều sử chung một tài khoản, thông thường các tổ chức dễ rơi vào tình trạng chia sẻ tài khoản riêng bừa bãi, dẫn đến mất kiểm soát trong quá trình quản trị tài khoản.

Hiện nay mỗi cán bộ phụ trách nhiều thiết bị quản trị trong cùng 1 hạ tầng IT họ phải lưu giữ nhiều mật khẩu, với N nhân viên IT và N thiết bị, số lượng tài khoản cần cấp cũng lên đến $N \times N$ tài khoản.



2. Giải quyết vấn đề điều chuyển tài khoản quản trị khi có sự thay đổi nhân sự

Hiện nay trong các cơ quan, việc nhân sự IT được điều điều chuyển công tác là điều không tránh khỏi, tuy nhiên trưởng bộ phận IT thường bị động trong việc “điều chuyển” tài khoản quản trị, dẫn tới tình trạng người cũ có thể vẫn còn quyền truy cập vào tài khoản quản trị cấp cao từ xa, trong khi đã chuyển công tác. Điều này dẫn đến mất kiểm soát an ninh cho hệ thống mạng của cơ quan, doanh nghiệp.



3. Không có kế hoạch thay đổi password định kỳ cũng như kiểm soát đảm bảo được thực hiện đúng

Một tài khoản quản trị nhiều khi cho phép chúng ta đặc quyền truy cập từ xa vào hệ thống, muốn được an toàn người quản trị cần định kỳ thay đổi mật khẩu để tránh sự nhòm ngó từ các tin tặc hay sự truy cập trái phép của nhân viên cũ.

Việc này không có gì phức tạp đối với hệ thống nhỏ chỉ có 1, 2 thiết bị. Tuy nhiên với 1 hệ thống lớn, rất đa dạng thiết bị như hệ thống CNTT của [Client] thì đó là điều không dễ dàng để triển khai thường xuyên và cần phải đảm bảo tiêu chuẩn bảo mật chung, và tiêu chuẩn bảo mật của thiết bị, cơ quan mình.

4. Truy vết hệ thống khi có sự cố.

Khi hệ thống bị mất dữ liệu, sai cấu hình, có lỗ hổng trong chính sách bảo mật gây mất an toàn cho hệ thống, sẽ mất rất nhiều thời gian để truy vết người gây ra sự cố, vì với những hệ thống lớn, mỗi quản trị viên sẽ phụ trách 1 mảng, khi triển khai các thiết bị cần bắt tay hỗ trợ chéo nhau, trong tình trạng mật khẩu bị chia sẻ nhiều như hiện nay, sẽ rất khó khăn để tìm được ai là người đã vào thay đổi cấu hình gây ra sự cố mạng.

5. Phân quyền và quản lý đối tác, nhà thầu.

Nếu như 1 cán bộ của đối tác đến công tác tại cơ quan chúng ta, về mặt vật lý mọi người sẽ kiểm soát tốt với những chiếc thẻ ra vào, và chứng minh nhân dân để tại phòng bảo vệ, và trong thời gian làm việc tại cơ quan họ vô tình “bị giám sát” bởi cán bộ của cơ quan.

Nhưng nếu 1 đối tác triển khai dự án IT trong cơ quan vào hỗ trợ cấu hình hệ thống, cán bộ chuyên trách của cơ quan sẽ rất khó khăn để giám sát từng dòng lệnh mà đối tác đã gõ, hay những thay đổi trong cấu hình thiết bị của cơ quan. Điều đó được thể hiện qua con số **58% các doanh nghiệp, hay cơ quan lo ngại rằng họ đã bị các đối tác vi phạm chính sách bảo mật hạ tầng mạng của mình ở trên**

Nhiều lúc chính nhà thầu, đối tác này vẫn còn nguyên quyền truy cập vào quản trị thiết bị sau khi họ rời cơ quan, vì mật khẩu cũ họ được cấp chưa được thu hồi hoặc thay đổi. Và số lượng đối tác càng lớn nguy cơ này xảy ra càng cao.

1.5. Các rủi ro và đe dọa từ tài khoản đặc quyền

- **Thiếu khả năng hiển thị và nhận thức của người dùng, tài khoản, tài sản và thông tin đăng nhập đặc quyền:** Nhiều tài khoản đặc quyền bị lãng quên từ lâu thường nằm rải rác trong các tổ chức. Những tài khoản này có thể cung cấp các cửa hậu nguy hiểm cho những kẻ tấn công, bao gồm, trong nhiều trường hợp, các nhân viên cũ đã rời công ty nhưng vẫn giữ quyền truy cập.
- **Cung cấp quá mức các đặc quyền :** Nếu các điều khiển truy cập đặc quyền bị hạn chế quá mức, chúng có thể phá vỡ quy trình làm việc của người dùng, gây ra sự thất vọng và cản trở năng suất. Vì người dùng cuối hiếm khi phàn nàn về việc sở hữu quá nhiều đặc quyền, dó đó quản trị viên CNTT thậm chí người dùng cuối thường được cung cấp quá nhiều đặc quyền. Ngoài ra, do quá trình luân chuyển công việc hoặc do các phát sinh đột suất, các nhân viên quản trị ngày càng có nhiều đặc quyền trong đó có các đặc quyền mà họ không còn sử dụng hoặc yêu cầu.
- **Những đặc quyền quá mức này làm tăng đáng kể nguy cơ phần mềm độc hại hoặc tin tặc có thể đánh cắp mật khẩu hoặc cài đặt mã độc có thể được gửi qua lướt web hoặc đính kèm email.** Phần mềm độc hại hoặc tin tặc sau đó có thể tận dụng toàn bộ các đặc quyền của tài khoản, truy cập dữ liệu của máy tính bị nhiễm và thậm chí tiến hành một cuộc tấn công chống lại các máy tính hoặc máy chủ được nối mạng khác.
- **Tài khoản và mật khẩu được chia sẻ :** Các nhóm CNTT thường chia sẻ root, Quản trị viên Windows và nhiều thông tin đặc quyền khác để thuận tiện để khởi động công việc và nhiệm vụ có thể được chia sẻ liền mạch khi cần. Tuy nhiên, với nhiều người chia sẻ cùng 1 mật khẩu tài khoản, có thể không thể ràng buộc các hành động được thực hiện với một tài khoản với một cá nhân. Điều này tạo ra các vấn đề bảo mật, kiểm toán và tuân thủ.
- **Thông tin được mã hóa cứng / nhúng :** Cần có thông tin đặc quyền để tạo điều kiện xác thực cho các giao tiếp và truy cập từ ứng dụng đến ứng dụng (A2A) và ứng dụng đến cơ sở dữ liệu (A2D). Các ứng dụng, hệ thống, thiết bị mạng và thiết bị IoT, thường được vận chuyển và thường được triển khai với các thông tin xác thực được nhúng, có thể đoán được và dễ gặp rủi ro. Ngoài ra, nhân viên thường sẽ giữ bí mật mã hóa cứng trong văn bản đơn giản, chẳng hạn như trong tập lệnh, mã hoặc tệp, do đó có thể dễ dàng truy cập khi họ cần.
- **Quản lý thông tin xác thực thủ công và / hoặc phi tập trung :** Các tài khoản và thông tin đặc quyền có thể được quản lý phi tập trung, dẫn đến việc thực thi không nhất quán các chính sách bảo mật tài khoản đặc quyền. Các quy trình quản lý đặc quyền không thể thực thi hiệu quả trong các môi

trường CNTT nơi có thể tồn tại hàng nghìn tài khoản, thậm chí hàng triệu tài khoản, thông tin và tài sản đặc quyền. Với rất nhiều hệ thống và tài khoản để quản lý, con người luôn sử dụng các phím tắt, chẳng hạn như sử dụng lại thông tin đăng nhập trên nhiều tài khoản và tài sản. Do đó, một tài khoản bị xâm nhập có thể gây nguy hiểm cho tính bảo mật của các tài khoản khác có chung thông tin đăng nhập.

- **Thiếu khả năng hiển thị các đặc quyền của tài khoản dịch vụ và ứng dụng:** Các ứng dụng và tài khoản dịch vụ thường tự động thực thi các quy trình đặc quyền để thực hiện các hành động, cũng như để liên lạc với các ứng dụng, dịch vụ, tài nguyên khác, v.v. và cũng bị các thiếu sót an ninh nghiêm trọng khác.
- **Các công cụ và quy trình quản lý danh tính im lặng :** Các môi trường CNTT hiện đại thường chạy trên nhiều nền tảng (ví dụ: Windows, Mac, Unix, Linux, v.v.) - mỗi môi trường được duy trì và quản lý riêng biệt. Thực tiễn này tương đương với quản trị CNTT không nhất quán, tăng thêm độ phức tạp cho người dùng cuối và tăng rủi ro không gian mạng.

2. TỔNG QUAN VỀ GIẢI PHÁP QUẢN TRỊ ĐẶC QUYỀN (PRIVILEGED ACCESS MANAGEMENT – PAM)

Trong những năm gần đây, thuật ngữ PRIVILEGED ACCESS MANAGEMENT - PAM thường xuyên được được các tổ chức về an ninh mạng đưa lên **vị trí số 1 trong top 10 dự án bảo mật CNTT** và khuyến cáo các giám đốc IT, hay những người lãnh đạo trong lĩnh vực này cần triển khai tại các hội nghị về quản lý rủi ro và bảo mật không gian mạng.

(Gartner – một công ty có trụ sở tại Mỹ - là một công ty hàng đầu về tư vấn và nghiên cứu toàn cầu cung cấp thông tin, tư vấn và công cụ cho các nhà lãnh đạo về CNTT)



Neil MacDonal, Phó chủ tịch và là chuyên gia của Gartner phân tích và giải thích về top 10 dự án bảo mật cho các Giám đốc an ninh mạng tại hội nghị về quản lý rủi ro và bảo mật không gian mạng, do Gartner tổ chức năm 2018

Dự án số 1: Giải pháp quản lý tài khoản đặc quyền

Triển khai giải pháp PAM nhằm ngăn chặn những kẻ tấn công hướng vào các tài khoản đặc quyền, đồng thời cho phép đội ngũ an ninh mạng giám sát được những truy cập bất thường trong hệ thống mạng. Ít nhất, những người đứng đầu trong đội ngũ quản lý an ninh mạng cần có phương tiện để thực hiện xác thực đa yếu tố đối với tất cả các quản trị viên. Tôi cũng khuyến cáo những giám đốc an ninh mạng nên sử dụng phương thức xác thực đa yếu tố đối với các đối tác hoặc nhà thầu truy cập vào quản trị hạ tầng mạng của cơ quan.

Gợi ý: Giai đoạn đầu các công ty cần tập trung vào những hệ thống tiềm ẩn rủi ro cao (Giá trị càng cao thì rủi ro càng nhiều) bằng cách giám sát hành vi của các đối tác truy cập vào hệ thống.

Nguồn: <https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2018>

GARTNER: TOP 10 DỰ ÁN BẢO MẬT THÔNG TIN NĂM 2019



Project 1: Privileged access management (PAM)

Privileged accounts (or administrative or highly empowered accounts) are attractive targets for attackers. A PAM project will highlight necessary controls to apply to protect these accounts, which should be prioritized via a risk-based approach. PAM projects should cover human and nonhuman system accounts and support a combination of on-premises, cloud and hybrid environments, as well as APIs for automation.

Dự án số 1: Giải pháp quản lý tài khoản đặc quyền (PAM)

Tài khoản đặc quyền (Hay các tài khoản có quyền lực cao, các tài khoản quản trị hệ thống) là đối tượng ưa thích của những kẻ tấn công. Một dự án PAM thực sự cần thiết để quản lý và bảo vệ những tài khoản này, nó cần được ưu tiên triển khai để kiểm soát được những rủi ro. Các dự án PAM sẽ giúp cơ quan quản lý các tài khoản của người dùng và các tài khoản máy, nó cần triển khai ngay trong cơ quan, môi trường đám mây hoặc kết hợp giữa 2 môi trường trên, cũng như triển khai tại các giao diện lập trình ứng dụng tự động.

Nguồn:

<https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2019/>

2.1. Giải pháp PAM là gì

Giải pháp PAM: viết tắt của Privileged Access Management: Giải pháp quản lý truy cập đặc quyền.

PAM là giải pháp giúp các tổ chức cung cấp truy cập tới các thiết bị trọng yếu trong tổ chức, tuân thủ các tiêu chuẩn, yêu cầu về quản lý và giám sát các tài khoản đặc quyền. Giải pháp PAM cung cấp các tính năng cho phép những nhà quản trị về rủi do và an ninh mạng sử dụng trong các trường hợp sau:

- ✓ Kiểm tra và quản lý tất cả các tài khoản đặc quyền của các thiết bị, ứng dụng trong hệ thống.
- ✓ Cho phép quản lý, tạo ngẫu nhiên các mật khẩu (lưu trong “Vault” – Kho lưu trữ mật khẩu bảo mật) và các thông tin xác thực khác cho các tài khoản sử dụng truy cập vào: các ứng dụng, dịch vụ hay sử dụng để quản trị, một cách tự động hóa.
- ✓ Kiểm soát truy cập vào các tài khoản đặc quyền, bao gồm các tài khoản dùng chung và các tài khoản khẩn cấp
- ✓ Cô lập, giám sát, ghi lại và kiểm toàn các phiên truy cập, các dòng lệnh và mọi hành động đã thực hiện sau khi truy cập vào thiết bị.

Nếu ví môi trường mạng như môi trường làm việc của một cơ quan, thì hệ thống **PAM** được ví như **Nhân viên bảo vệ và Hệ thống camera giám sát** trong cơ quan của bạn.

Quản lý truy cập đặc quyền (PAM) bao gồm các chiến lược và công nghệ để kiểm soát quyền truy cập và quyền truy cập nâng cao (đặc quyền) cho người dùng, tài khoản, quy trình và hệ thống trên môi trường CNTT.

Mặc dù quản lý đặc quyền bao gồm nhiều chiến lược, mục tiêu trọng tâm của PAM là thực thi đặc quyền tối thiểu, được xác định là hạn chế quyền truy cập và quyền cho người dùng, tài khoản, ứng dụng, hệ thống, thiết bị (như IoT) và quy trình tính toán đến mức tối thiểu cần thiết để thực hiện các hoạt động thường xuyên, ủy quyền.

PAM đã thay đổi mạnh mẽ cách các tổ chức bảo vệ quyền truy cập vào các hệ thống quan trọng. Sử dụng kho xác thực (credentials vault, password vault) và các công cụ kiểm soát phiên truy cập, PAM đã cho phép các nhà quản lý cho phép truy cập đặc quyền trong khi giảm thiểu đáng kể nguy cơ thâm nhập gây tổn hại

an ninh của hệ thống. Bằng cách tập trung thông tin đăng nhập đặc quyền ở một nơi, các hệ thống PAM có thể đảm bảo mức độ bảo mật cao cho họ, kiểm soát ai đang truy cập chúng, đăng nhập tất cả các truy cập và theo dõi mọi hoạt động đáng ngờ.

2.1.1 Lợi ích của giải pháp PAM

Việc thực hiện quản lý đặc quyền không chỉ giảm thiểu khả năng vi phạm an ninh xảy ra, mà còn giúp hạn chế phạm vi vi phạm nên xảy ra.

Một điểm khác biệt giữa PAM và các loại công nghệ bảo mật khác là PAM có thể phá hủy nhiều điểm của chuỗi tấn công mạng, cung cấp sự bảo vệ chống lại cả cuộc tấn công bên ngoài cũng như các cuộc tấn công vào mạng và hệ thống.

PAM cung cấp một số lợi ích chính, bao gồm:

- **Hạn chế các hướng tấn công và khai thác tài khoản đặc quyền:**
- **Giảm lây nhiễm và lan truyền phần mềm độc hại :** Nhiều loại phần mềm độc hại (như SQL Injection, dựa trên việc thiếu đặc quyền tối thiểu) cần các đặc quyền nâng cao để cài đặt hoặc thực thi. Loại bỏ các đặc quyền quá mức, chẳng hạn như thông qua việc thực thi đặc quyền tối thiểu trên toàn tổ chức, có thể ngăn phần mềm độc hại có được chở đứng hoặc giảm sự lây lan của nó nếu có.
- **Hiệu suất hoạt động được nâng cao:** Hạn chế các đặc quyền trong phạm vi tối thiểu của các quy trình để thực hiện một hoạt động được ủy quyền giúp giảm khả năng xảy ra sự cố không tương thích giữa các ứng dụng hoặc hệ thống và giúp giảm nguy cơ ngừng hoạt động.
- **Dễ dàng đạt được và chứng minh sự tuân thủ:** Bằng cách hạn chế các hoạt động đặc quyền có thể được thực hiện, quản lý truy cập đặc quyền giúp tạo ra một môi trường ít phức tạp hơn và do đó, thân thiện với kiểm toán hơn.

2.1.2 Các tính năng của PAM

1. Kiểm soát thông tin và trao quyền ra vào hệ thống

Mỗi khi có người muốn truy cập vào hệ thống thì quy trình cấp mật khẩu vào làm việc tương tự như những người vào trong cơ quan liên hệ công tác.

- ✓ Nếu như bạn vào cơ quan nào công tác bạn cần khai báo đầy đủ các thông tin cá nhân, liên hệ với phòng ban nào, thời gian làm việc bao lâu, nếu xác nhận thông tin chính xác bạn sẽ được nhân viên bảo vệ cấp **thẻ ra vào** để làm việc trong cơ quan. Đồng thời bạn phải cam kết chấp hành các quy định chung của pháp luật cũng như của chính cơ quan đó.
- ✓ Thì ở đây sau khi khai báo đầy đủ thông tin về cá nhân, các ứng dụng thiết bị cần truy cập và nội dung công việc cần làm trên thiết bị, nếu chính xác bạn được người quản trị hệ thống cấp cho **tài khoản “tạm thời”** để truy cập vào hệ thống. Khi truy cập vào hệ thống bạn cần cam kết những quy định chung về chính sách bảo mật, cũng như quy định riêng của phòng IT đó.



2. Theo dõi và ghi lại mọi hành vi khi đăng nhập vào cấu hình hệ thống

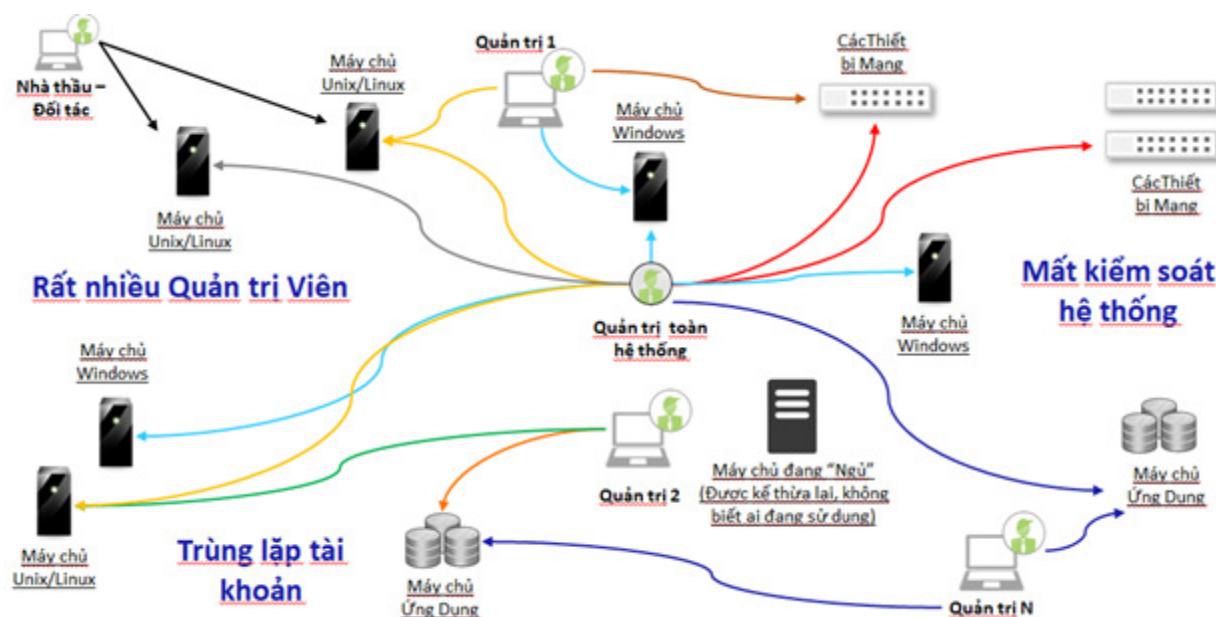
- Tuy nhiên nếu chỉ kiểm soát vòng ngoài không thì chưa đủ, chúng ta cần biết những đối tác, hay nhân viên trong cơ quan đang làm gì trong hệ thống của mình, khi đăng xuất xong việc họ đã thay đổi gì về mặt cấu hình thiết bị. Vì vậy giải pháp PAM cung cấp 1 hệ thống **ghi lại và kiểm toán** toàn bộ thao tác của mọi người khi truy cập vào hệ thống giống như 1 **hệ thống Camera an ninh** trong cơ quan.



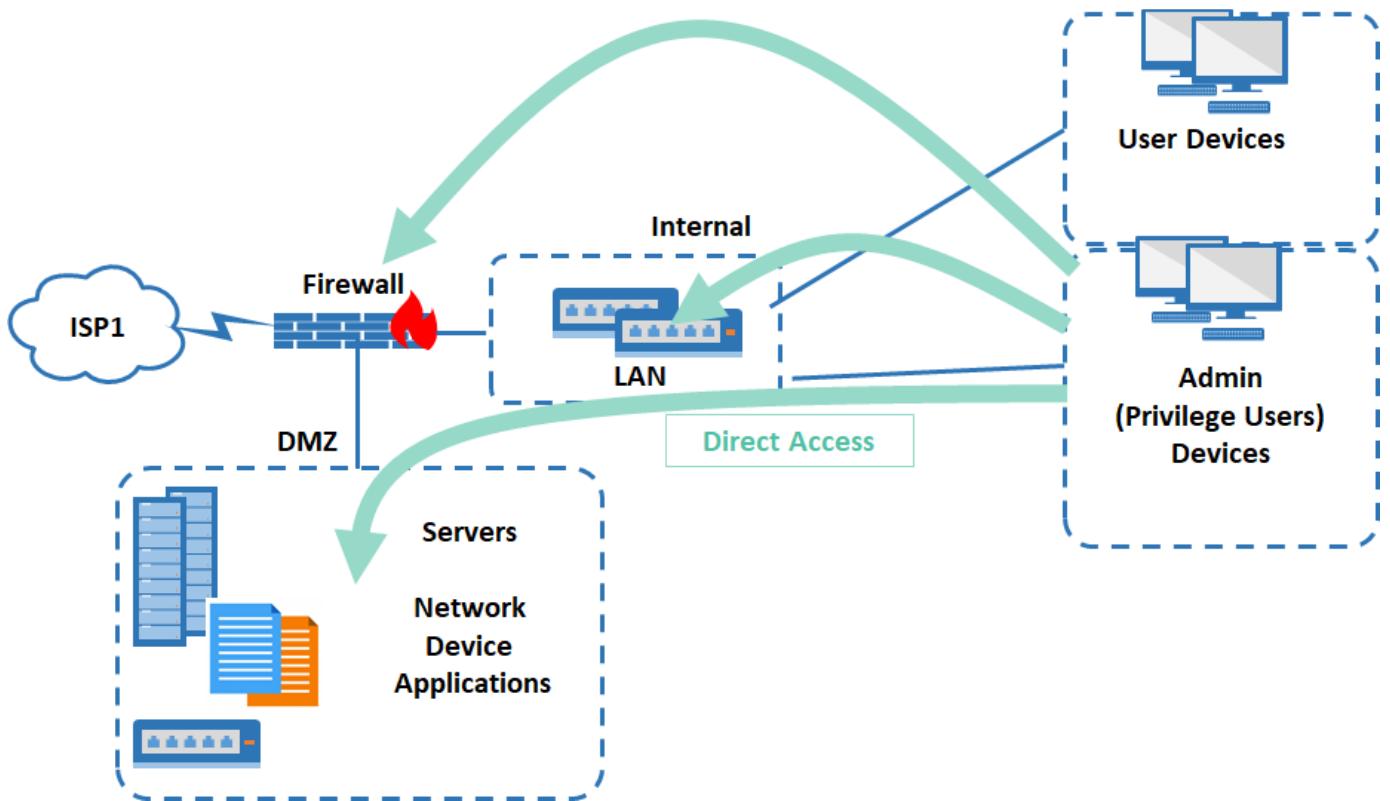
2.2. Giải pháp PAM hoạt động như thế nào.

Dưới đây là 2 mô hình cơ bản của 1 cơ quan, doanh nghiệp trước và sau khi sử dụng giải pháp PAM.

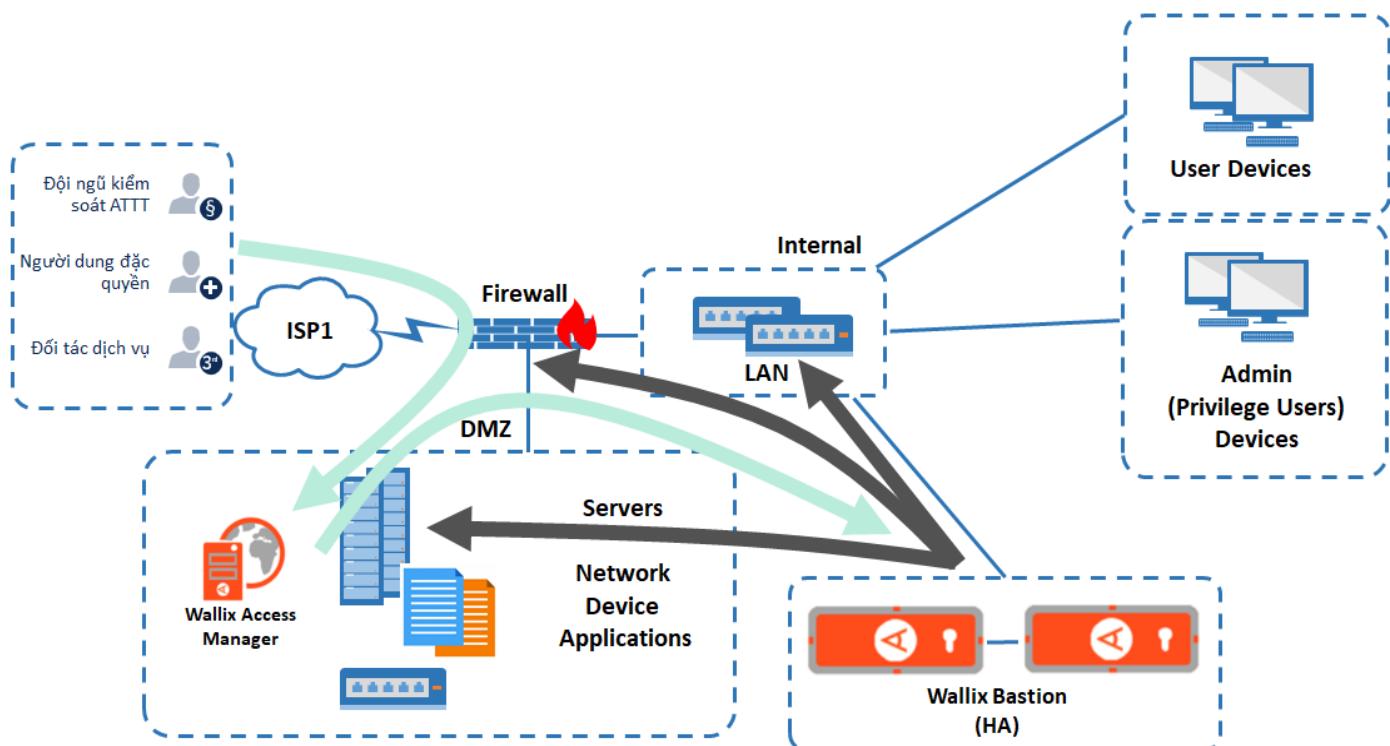
Trước khi sử dụng giải pháp PAM, Giám đốc, trưởng phòng IT sẽ rất khó khăn trong việc phân hoặc và cấp quyền cho các đối tác, nhà thầu và quản trị viên như hình dưới, công việc quản trị sẽ rất phức tạp và hỗn loạn.



Và sau khi sử dụng giải pháp PAM, các hệ thống đều qua 1 thiết bị kiểm soát, phân quyền chung, việc phân quyền này được quản lý bằng cơ chế, chính sách rõ ràng:

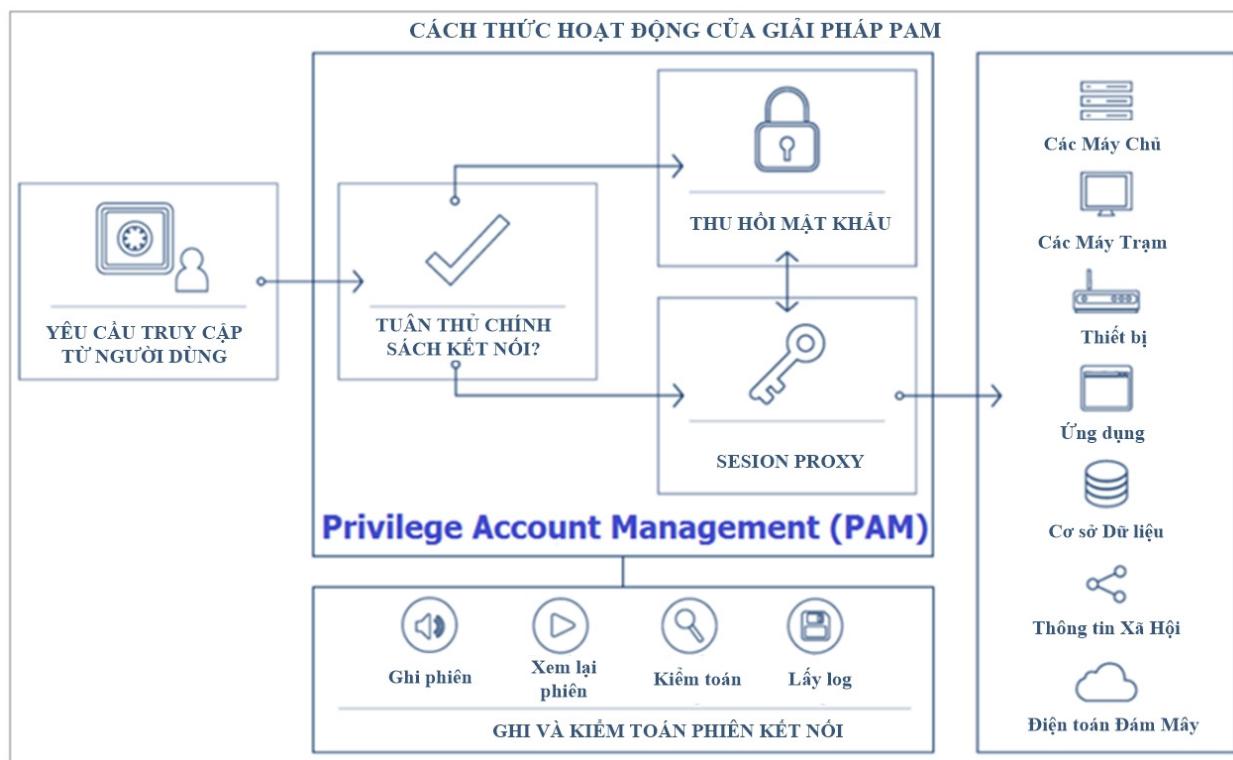


Kết nối khi chưa có hệ thống PAM



Kết nối quản trị qua hệ thống PAM

2.3. PAM GIẢI QUYẾT VẤN ĐỀ GÌ CHO HẠ TẦNG



Giải pháp PAM được cung cấp nhằm đáp ứng những mục tiêu sau:

- Giúp bảo vệ các tổ chức khỏi các mối đe dọa nội bộ do lạm dụng quyền truy cập của người dùng đặc quyền đồng thời cũng giúp các tổ chức đáp ứng các quy định nghiêm ngặt về bảo mật cũng như tiêu chuẩn bảo mật cần tuân thủ.
- Kiểm soát và theo dõi người dùng đặc quyền của mình khi họ truy cập vào máy chủ của bạn (Windows, Unix / Linux, v.v.) : không chỉ phần cứng mạng mà cả các ứng dụng của bạn (VMware ESX, Oracle, MySQL, v.v.).
- Cho phép Giám đốc, trưởng phòng IT giám sát các phiên làm việc của nhân viên IT, đối tác theo thời gian thực, xem lại chúng khi cần thiết (Kiểm toán, tai nạn, hay sự cố liên quan tới pháp luật...).
- Hệ thống có thể liên kết bất cứ 1 kết nối nào tới 1 tài khoản chung (ví dụ tài khoản Root) với 1 người dùng đã được định danh – do đó mang lại sự đảm bảo về trách nhiệm trong cả kết nối lẫn hành động của tài khoản.
- Được sử dụng để cung cấp cho các nhà cung cấp dịch vụ bên ngoài quyền truy cập vào hệ thống thông tin đồng thời đảm bảo mức độ bảo mật và truy vết nguồn gốc tuyệt vời.
- Giải pháp PAM cung cấp đảm bảo tuân thủ các tiêu chuẩn và quy định hiện hành và tương lai.
- Giải pháp PAM có tính năng như kết nối thiết bị tự động và chức năng đăng nhập một lần (SSO) đảm bảo rằng các nhóm vận hành và bảo trì sẽ cảm thấy đơn giản và dễ dàng sử dụng.
- Ngoài ra, giải pháp PAM hoàn toàn có thể tích hợp vào các cơ sở hạ tầng quản lý người dùng hiện có như: Active Directory, LDAP, RADIUS, v.v. để xác thực người dùng.

3. ĐỊNH HƯỚNG LỰA CHỌN GIẢI PHÁP

3.1. ĐỊNH HƯỚNG LỰA CHỌN GIẢI PHÁP

Với những thực tại cần giải quyết cho vấn đề quản lý truy cập đặc quyền, và với công việc đặc thù của [Client] chúng tôi xin đề xuất giải pháp của hãng với tiêu chí như sau:

- Đây phải là hãng có thương hiệu lớn trên thế giới được đơn vị tư vấn thế giới xếp hàng sản phẩm “**Product leader**” – sản phẩm thương hiệu hàng đầu trên bản đồ thị trường giải pháp PAM của thế giới
- Hãng này được đánh giá cao về tính bảo mật và khả năng tương thích với hệ thống hiện hành (các thiết bị và ứng dụng đa dạng, phong phú) của [Client]
- Giải pháp triển khai phải đơn giản, nhanh gọn, không làm ảnh hưởng, thay đổi kêt cấu hạ tầng CNTT hiện có của [CLIENT].

3.2. GIẢI PHÁP ĐỀ XUẤT

Đáp ứng những yêu cầu nêu trên Chúng tôi xin đề xuất giải pháp quản lý đặc quyền PAM của hãng **WALLIX**, giải pháp có tên gọi **Wallix Bastion**, giải pháp này cho phép [CLIENT] quản lý và phân quyền quản trị hiệu quả, đồng thời giải quyết được tất cả những vấn đề đang tồn tại trong quá trình quản lý phân quyền truy cập tại [CLIENT].

Chúng tôi xin đề xuất giải pháp của hãng Wallix vì những lý do sau:

3.2.3 Thương hiệu và uy tín – là giải pháp hàng đầu thế giới

Nhà phân tích **KuppingerCole**, được thành lập năm 2004, là một tổ chức phân tích quốc tế và độc lập có trụ sở tại châu Âu. Công ty chuyên cung cấp tư vấn trung lập, chuyên môn, lãnh đạo tư duy và sự phù hợp thực tế trong An toàn thông tin, Nhận dạng & Quản lý truy cập (IAM), Quản trị (IAG), Quản lý rủi ro & Tuân thủ (GRC) cũng như tất cả các lĩnh vực liên quan đến Chuyển đổi kỹ thuật số.

KuppingerCole Analysts đã nhận định về giải pháp PAL – WALLIX Bastion như sau:

- ✓ Wallix được các nhà phân tích của **KuppingerCole** xếp hạng vào nhóm dẫn đầu thị trường thế giới “Product leader” về thị trường giải pháp PAM dựa trên các tiêu chí: Tính năng và năng lực của sản phẩm/ Dịch vụ cung cấp.
- ✓ Wallix đã được xác nhận triển khai rộng rãi tại thị trường: Châu Âu, và Trung Đông.
- ✓ Wallix được ghi nhận với những thế mạnh về: tính bảo mật, chức năng, khả năng tương thích và mức độ hòa hợp với các hệ thống hiện hành cũng như sự hữu ích của hệ thống mang lại. cụ thể như sau:
 - Cho phép triển khai rộng rãi và trên nhiều nền tảng thiết bị, ứng dụng khác nhau
 - Tính năng quản lý phiên truy cập đứng đầu thế giới: sử dụng công nghệ thiết lập các phiên kết nối quản trị đặc quyền từ tài khoản quản trị tới hệ thống đích: bao gồm các tính năng giám sát và kiểm toán các hành vi truy cập đặc quyền, công cụ này cũng cho phép cung cấp các cơ chế SSO (single sign on) cho phép người dùng đăng nhập 1 lần để truy cập vào nhiều ứng dụng thiết bị tại 1 thời điểm.
 - Hỗ trợ tính năng Công truy cập web và chỉ sử dụng 1 công cụ quản trị tập trung duy nhất cho tất cả các mô đun triển khai
 - Hỗ trợ cơ chế Multi Tenancy và cơ chế dự phòng HA



- Có lộ trình phát triển sản phẩm với tính khả thi cao.

3.2.4 Giới thiệu về WALLIX



WALLIX
TRACE, AUDIT & TRUST

Wallix được thành lập vào năm 2003, là công ty **đi đầu trong giải pháp phần mềm bảo mật CNTT** với mục đích quản lý **an ninh mạng và cơ sở hạ tầng CNTT trọng yếu**. Wallix là công ty của Châu Âu, có trụ sở và văn phòng đại diện ở Pháp, Anh, Mỹ với nhiều đối tác trên khắp Châu Âu, Đông Nam Á và Nga.

Hiện đã có trên **200 công ty, tổ chức và cơ quan thuộc khối chính phủ** tin dùng sản phẩm của Wallix cho giải pháp bảo mật CNTT của Wallix

Các sản phẩm của WALLIX cho phép người dùng thích nghi và tuân thủ các tiêu chuẩn ISO27001, PCI, SOX và PSN (Mạng dịch vụ công cộng), v.v. về bảo mật thông tin và dữ liệu, đồng thời đảm bảo tính toàn vẹn hệ thống của họ trong qua trình truy vết mọi hoạt động trên hệ thống CNTT.

WALLIX đã được Cơ quan bảo mật Thông tin và Mạng của Pháp (**ANSSI**) kiểm tra và đạt được Chứng nhận Bảo mật Tiêu chuẩn Chung (**CSPN**), Chứng nhận Tiêu chuẩn Chung: **CCRA**. Đồng thuận về tiêu chuẩn chung mới nhất được áp dụng kể từ ngày 8 tháng 9 năm 2014. BASTION cũng được cấp chứng chỉ FSTEK đầy đủ của Nga. Với những chứng chỉ này, BASTION hiện đang được sử dụng trong một số lĩnh vực đặc thù như: các **cơ quan của lực lượng Cảnh sát và Bộ Quốc phòng** trên toàn cầu.



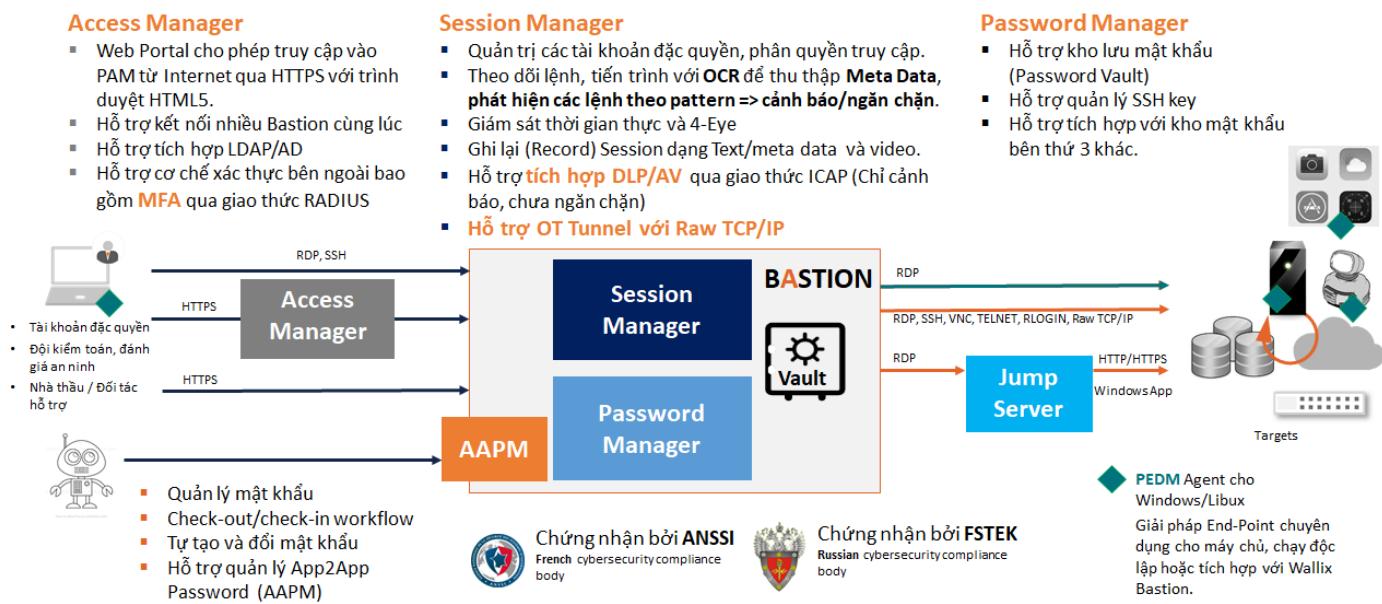
WALLIX đã phát triển bộ giải pháp WALLIX **BASTION**, một giải pháp PAM cho phép dễ dàng tích hợp vào hạ tầng IT của khách hàng, giải pháp cho phép khách hàng quản lý các thông tin về phân quyền quản trị như: “ Ai làm gì, khi nào, ở đâu và như thế nào”, bao gồm các thông tin về hành động người dùng, lưu trữ log, video theo thời gian thực.

Thông tin chi tiết tại: www.wallix.com/en

3.2.5 Giải pháp Wallix Bastion

Bộ giải pháp **Wallix Bastion** (Viết tắt là **WAB**) là giải pháp quản lý tập trung, cho phép bảo mật các truy cập đặc quyền, giám sát các phiên truy cập đặc quyền, các báo cáo kiểm toán tường minh và những thông số phân tích hành vi của người dùng đặc quyền là những căn cứ đáng tin cậy để ra quyết định ngăn cản những cuộc tấn công theo vết của họ, giúp giảm những mã độc lây lan trong hệ thống.

Giải pháp **WALLIX Bastion Suite** bao gồm các tính năng quản lý password (**Password Manager**), quản lý phiên truy cập (**Session Manager**) với nhiều tính năng mở rộng trên cùng 1 nền tảng.



3.2.5.1. Quản lý phiên truy cập (Session Manager)

Mô đun này cho phép quản lý các phiên người dùng giúp ngăn chặn rủi ro và kiểm soát truy cập theo thời gian thực.

- Quản lý và quản trị các tài khoản đặc quyền
 - o Hệ điều hành UNIX và Windows, các thiết bị mạng, cơ sở dữ liệu, hạ tầng thiết bị vật lý và thiết bị ảo hóa.
 - o Các ứng dụng vận hành, kinh doanh, và các máy trạm (ví dụ: quản lý firewall, các ứng dụng salesforce, sageforce)
 - o Truy cập trực tiếp và các tài nguyên sử dụng các máy trạm thụ động (Putty, winSCP, MSTC, OpenSSH...) với các chính sách kết nối được nhúng trực tiếp vào hệ thống Bastion
 - o Quy trình làm việc được thiết kế với các cấu hình truy cập liên quan đến ngữ cảnh.
- Giám sát toàn bộ hoạt động của người dùng đặc quyền: với các cảnh báo và các phiên từ xa có thể bị ngắt khi cần thiết: các chuỗi ký tự (Blacklist), báo cáo về cá sự kiện ứng dụng nhỏ, trình tự xử lý, luồng lưu lượng từ bàn phím, (“session Probe”, “4-Eyes”, OCR) hoặc việc sử dụng của những Source Server
- Thu thập Metadata (Session Probe): Có giao diện hiển thị chi tiết thông tin liên quan tới ngữ cảnh
- Quản lý APP từ xa

3.2.5.2. Quản lý mật khẩu. (Password Manager)

Mô đun này cho phép người quản trị quản lý các chính sách về mật khẩu và thực thi mật khẩu. Tính năng bảo mật được tăng cường bằng cách đảm bảo rằng người dùng chỉ có quyền truy cập vào các tài nguyên họ cần để làm việc. Điều này giúp đảm bảo các mật khẩu và khóa SSH sẽ không bị lộ hoặc sử dụng sai đối tượng:

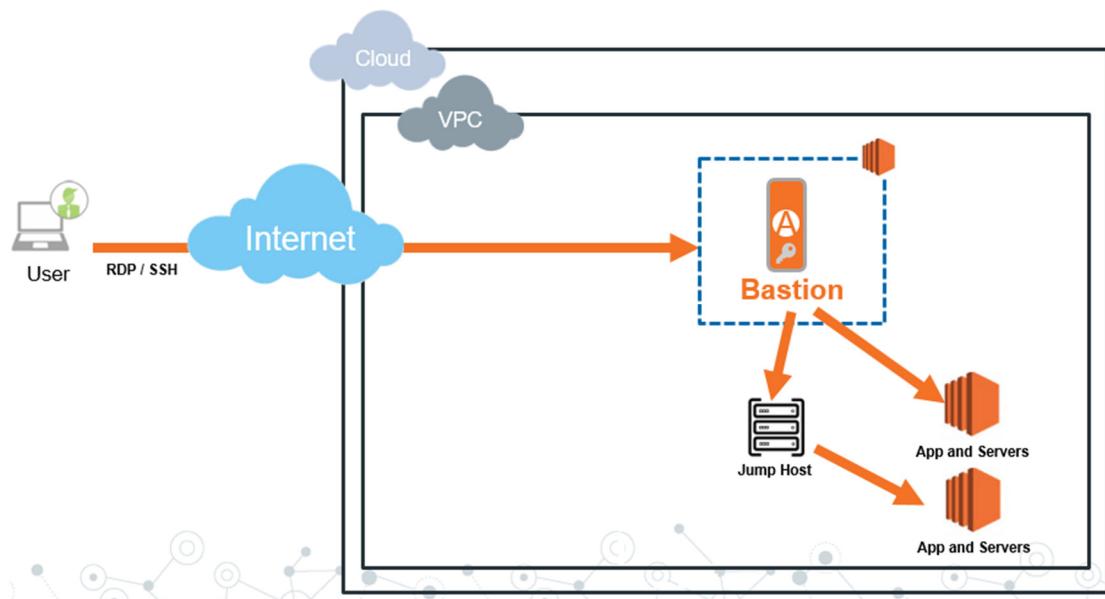
- Mật khẩu được lưu trữ an toàn và các khóa SSH được mã hóa trong “kho chứng thực”
- Định kỳ thay đổi mật khẩu
- Thư viện plugin chuyên dụng để quản lý mật khẩu mục tiêu
- Hỗ trợ chứng chỉ SSH
- Quản lý mật khẩu ứng dụng và quản lý tài khoản dịch vụ.

3.2.5.3. Các mô đun khác

3.2.5.3.1. Quản lý truy cập qua Web (Web Access Manager – WAM)

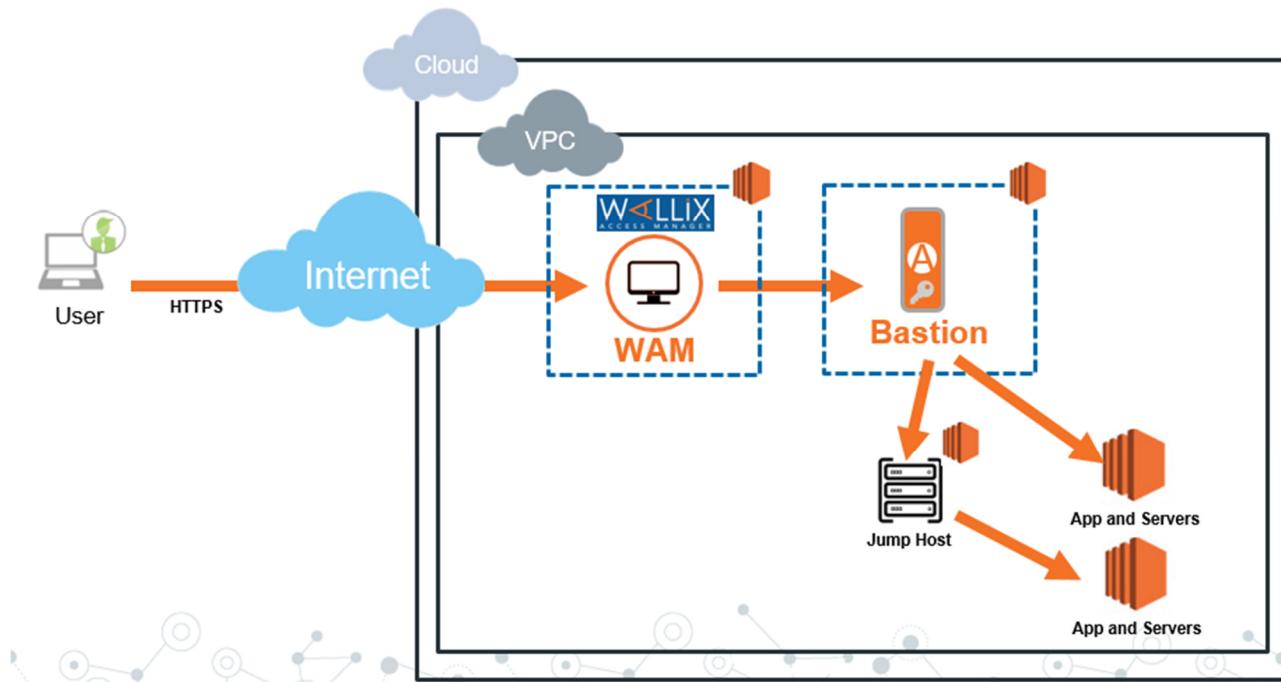
Người dùng trên Internet có thể truy cập vào hệ thống bên trong qua PAM bằng cách:

- Mở các cổng SSH và RDP ra ngoài Internet



- Phương thức trên không được khuyến khích sử dụng vì kém an toàn. Chúng ta có thể dùng
 - o Hoặc triển khai VPN để kết nối như các người dùng quản trị trong mạng nội bộ
 - o Wallix Bastion cung cấp mô đun Access Manager (WAM).

Quản lý truy cập Wallix Access Manager cung cấp web portal cho người dùng và quản trị.



Mô-đun WAM cho phép:

- Tìm kiếm toàn diện trên nền tảng hạ tầng Bastion của bạn.
- Tích hợp SSO (single sign-on) trên toàn bộ hệ thống Bastion sử dụng cấu trúc RDP và SSH.
- Bảo vệ thiết bị và hệ thống qua các bộ chính sách có thể tự động xác thực hoặc thu hồi quyền truy cập của người dùng
- Ủy quyền cho các hệ thống của đơn vị thứ ba để xác thực và nhận dạng người dùng (SAML 2.0).
- Kiến trúc Multi tenant tương thích với môi trường của nhà cung cấp dịch vụ, với các trường hợp được cô lập hoàn toàn
- Có giao diện web tùy chỉnh
- Không yêu cầu VPN để truy cập từ xa.

3.2.5.3.2. Kho mật khẩu (Password Vault)

Mô-đun này cho phép lưu trữ an toàn mọi thông tin đăng nhập lưu bên trong WALLIX Bastion.

Mọi dữ liệu nhạy cảm đều được mã hóa (chẳng hạn như thông tin đăng nhập của tài khoản đích, mật khẩu của người dùng cục bộ, kết nối giao diện web, kết nối proxy SSH và RDP, v.v.) bằng cách sử dụng thuật toán mật mã mạnh. Thuật toán này sử dụng khóa mã hóa bí mật và duy nhất cho WALLIX Bastion của bạn.

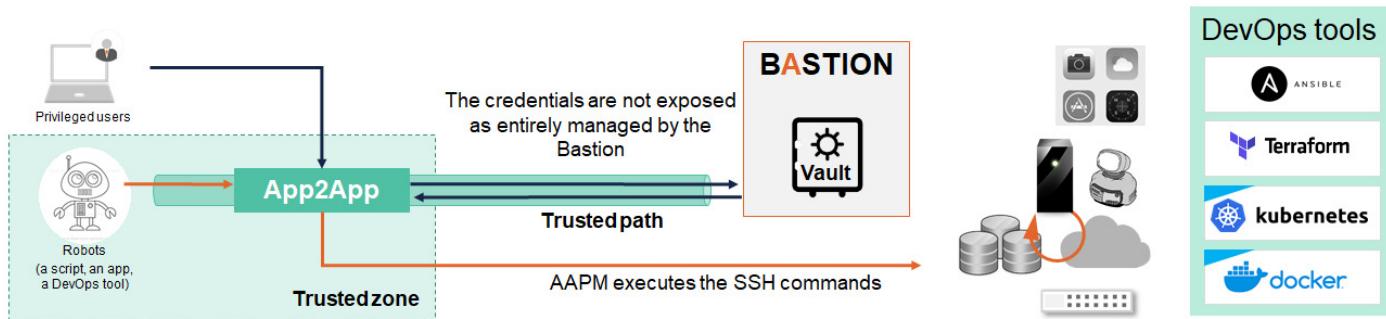
WALLIX cung cấp một phương pháp tiếp cận theo mô-đun để quản lý kho mật khẩu, do đó, mặc dù WALLIX Bastion chứa Vault của riêng nó, nhưng cũng có thể sử dụng một kho dữ liệu bên ngoài từ một nhà cung cấp khác (chẳng hạn như Cyberark hoặc Thycotic). Việc tích hợp sau đó cho phép sử dụng Quản lý phiên của WALLIX Bastion và một kho mật khẩu bên ngoài.

Hiện tại, WALLIX là nhà cung cấp duy nhất có thể tích hợp với kho mật khẩu của các nhà cung cấp khác.

3.2.5.3.3. AAPM

AAPM cung cấp khả năng tích hợp PAM cho DevOps





3.3. Các ưu điểm của giải pháp Wallix Bastion

- Wallix Bastion là một trong số ít giải pháp PAM được đóng gói hoàn thiện kết hợp với hệ điều hành (Hardened OS). Các mô đun chính được tích hợp vào và có thể kích hoạt trên cùng 1 máy chủ hoặc riêng tùy theo nhu cầu.

Dựa trên Linux Debian 8 (Jessie), WALLIX Bastion được tùy chỉnh (kernel linux 4.4) và được làm cứng bằng các bản vá GRSecurity. Các bản vá này cung cấp bảo vệ hệ thống sau đây:

- Bảo vệ Bộ nhớ (Memory Corruption Defenses) để đảm bảo hiệu suất cao trong khi vẫn bảo vệ chống lại Return Oriented Programming (ROP).
- Bảo vệ File System
- Và nhiều kỹ thuật phòng vệ khác chống process snooping, tự động tải các mô-đun lỗi dễ bị tổn thương, v.v.
- Kiểm soát truy cập dựa trên vai trò (RBAC), liên kết cho mỗi người dùng một vai trò xác định thao tác nào có thể được thực hiện trên các đối tượng nhất định, để đảm bảo quyền truy cập vào các tệp.
- Các plugin GCC để đảm bảo tính ổn định của ứng dụng và để chống lại việc khai thác tấn công Overflow và lỗ hổng kernel.

Nhờ đó, Wallix Bastion không yêu cầu khách hàng phải mua License cho hệ điều hành, Database, v.v.

- Wallix Bastion dùng cơ chế Agentless 100%. Các hệ thống đầu cuối được quản trị bởi PAM mà không cần cài đặt thêm bất kỳ phần mềm nào khác. Do đó Wallix Bastion hoàn toàn có thể dùng để quản lý các thiết bị chuyên dụng không cho phép cài đặt thêm phần mềm vào, chỉ cần các thiết bị chuyên dụng này hỗ trợ các giao thức quản trị chuẩn như SSH/Telnet/Rlogin/RDP/VNC.

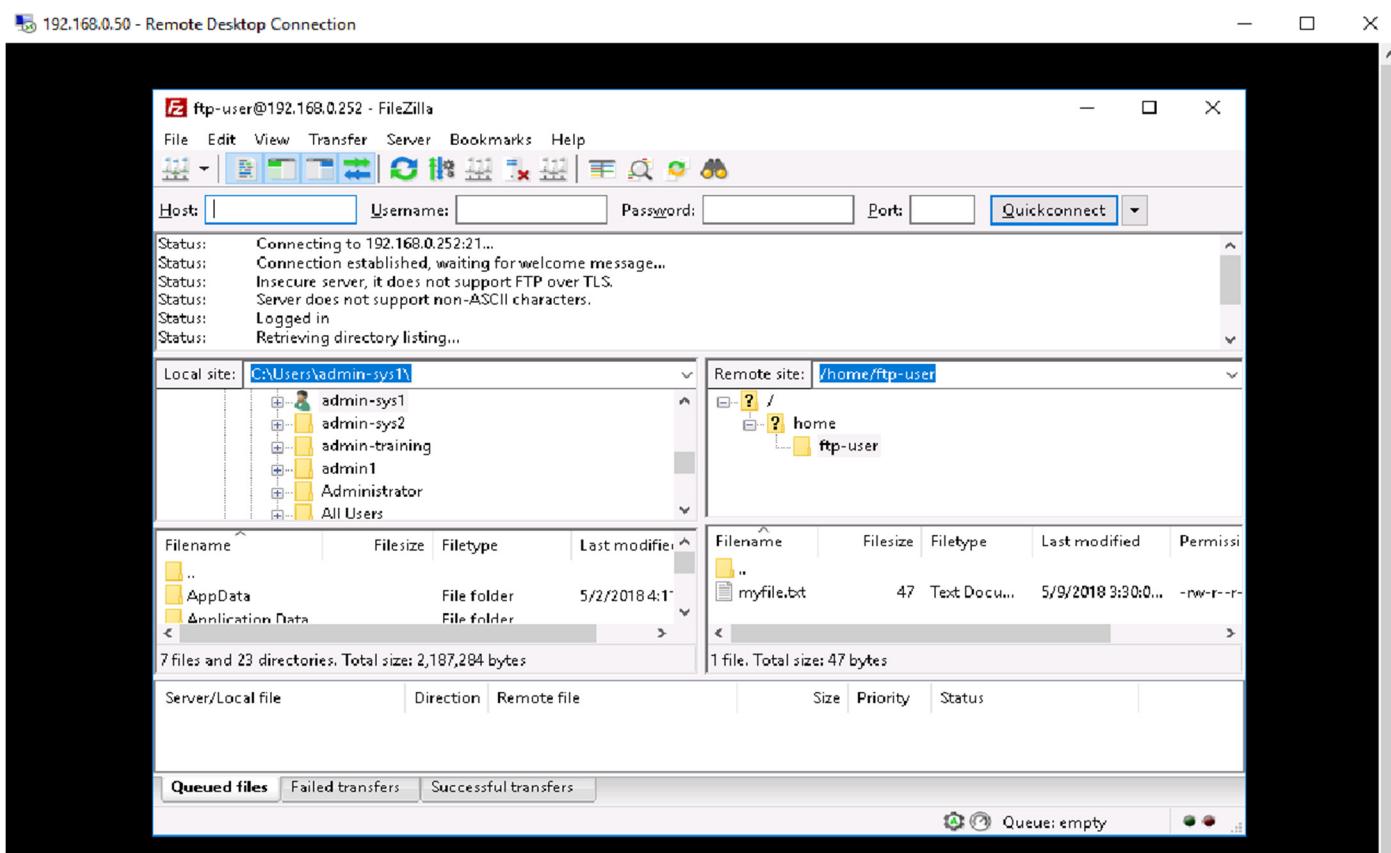
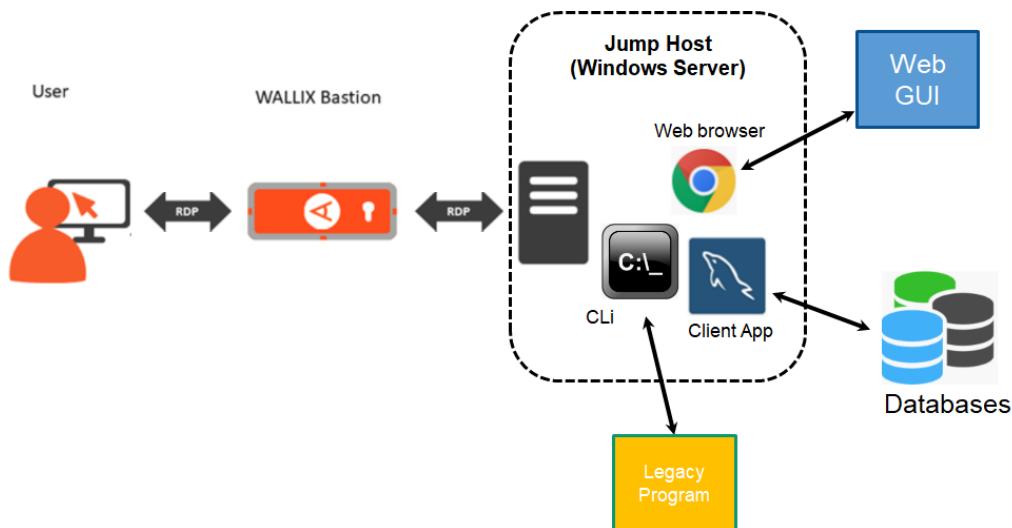
Hạn chế của phương thức agentless này là Wallix Bastion không thể can thiệp quá sâu vào các thao tác của người dùng đặc quyền, đặc biệt nếu người dùng đặc quyền kết nối vật lý trực tiếp vào hệ thống cần quản trị bằng bàn phím/chuột vật lý.

Các hạn chế này có thể giải quyết một phần bởi giải pháp PEDM (Privilege Elevation and Delegation Management) BestSafe của Wallix.

Ngoài ra, hệ thống cũng cần được cấu hình để hạn chế tối đa các kết nối trực tiếp bằng phương thức vật lý, ép buộc người dùng quản trị phải kết nối thông qua Wallix Bastion.



- Đối với các hệ thống sử dụng giao diện Web hoặc phần mềm chuyên dụng để quản trị, Wallix Bastion hỗ trợ kết nối thông qua máy tính trung gian được gọi là Jump Server. Jump Server này có thể chỉ là 1 máy tính cài Windows OS thông thường để chạy các phần mềm quản trị hoặc là Terminal Server cho phép các ứng dụng quản trị chạy dạng Remote Application. Nhờ đó, Wallix Bastion cho phép quản trị VMware, ESX, Database: Oracle, My SQL, MS SQL Server; v.v cũng như các ứng dụng đang phát triển khác, do đó đảm bảo xác thực trong kết nối và xác thực trong hành vi. Các phiên kết nối này được ứng xử như các phiên kết nối RDP với khả năng ghi Video, thu thập Metadata.



3.4. Bảo mật hệ thống

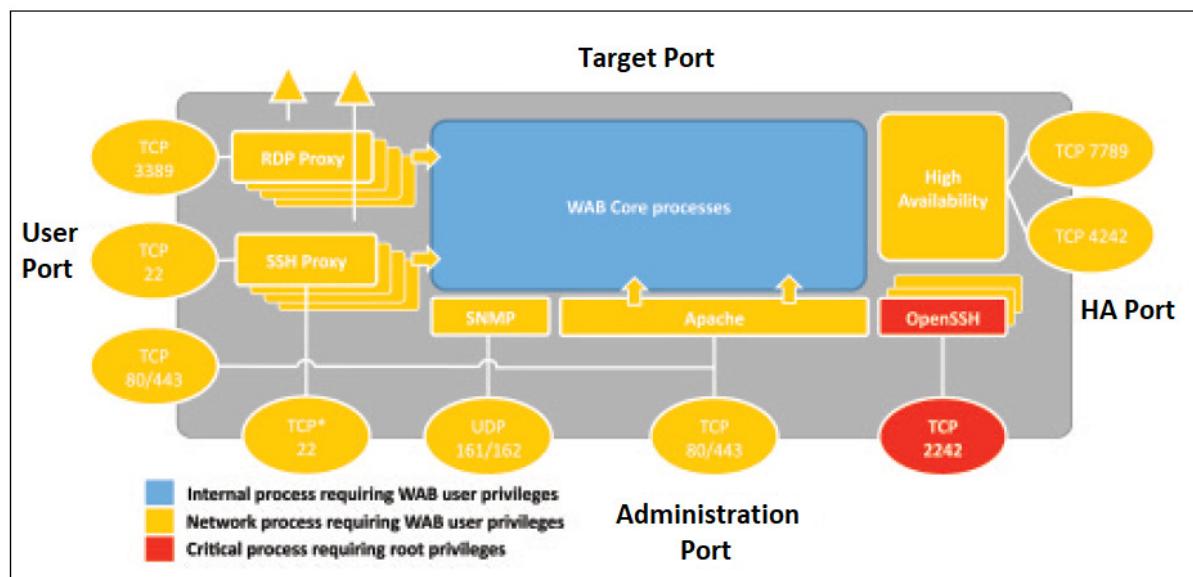
WALLIX Bastion là một giải pháp tập trung bảo đảm quyền truy cập đặc quyền và giám sát các phiên đặc quyền. Do vai trò và vị trí của nó trong cơ sở hạ tầng mạng, nó có thể đại diện cho một điểm Failure duy nhất và là mục tiêu chính cho những kẻ xâm nhập độc hại. Nhận thức đầy đủ về trách nhiệm bảo mật mạng của mình, WALLIX đã cung cấp nền tảng của Bastion để đảm bảo tính toàn vẹn của nó. Theo đó, WALLIX đã thực hiện một số quy trình cứng để đảm bảo sự mạnh mẽ của Bastion.

NGUYÊN TẮC RIÊNG TÙ

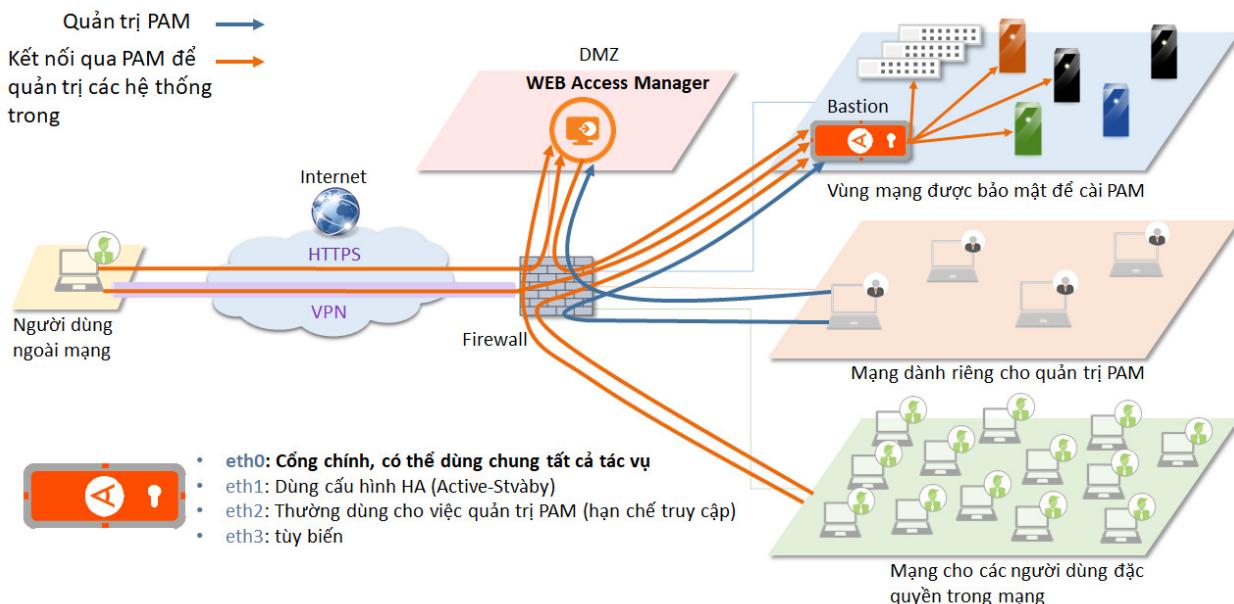
Tuyến phòng thủ đầu tiên để bảo vệ BASTION là đảm bảo rằng người dùng không thể thực thi các chương trình cũng như truy cập dữ liệu nằm ngoài phạm vi của họ. Với OS được tối ưu hóa và tích hợp chặt chẽ, trên Wallix Bastion, người dùng chỉ được cấp các quyền bắt buộc tối thiểu và có thể đạt được độ cao đặc quyền tạm thời bằng cách sử dụng lệnh sudo. Bằng cách này, họ không có quyền truy cập vào thông tin đăng nhập của quản trị viên mà vẫn có khả năng chạy các đặc quyền yêu cầu ứng dụng.

KHAI THÁC PORT

Wallix Bastion hạn chế quyền truy cập bên ngoài của nó vào bốn vai trò được xác định trước: Quản trị, HA, Target, Người dùng PAM. Các vai trò này được phân vùng thông qua kỹ thuật Cách ly cổng: Mỗi vai trò giao tiếp với Bastion thông qua một cổng chuyên dụng để chúng không thể truy cập các khả năng vai trò khác để có được các đặc quyền cao hơn cũng như bắt đầu lưu lượng truy cập ngang hàng trực tiếp.



Không chỉ thế, các vai trò này cũng có thể được chỉ định trên các card mạng khác nhau để đảm bảo cách ly cổng vật lý lẫn luận lý.



MÃ HÓA

Các biện pháp bảo vệ bằng mã hóa hiện đại được sử dụng để bảo vệ cho Wallix Bastion và các dữ liệu của hệ thống. Mật mã được triển khai cho người dùng và truy cập quản trị, cũng như để kết nối với các hệ thống đích.

Các thuật toán mã hóa được sử dụng bao gồm:

- HTTPS và SSH được sử dụng để quản trị.
- Thiết lập GUI / x509: Sử dụng TLS v1.2.
- Giao thức RDP:
 - TLS v1.2 với việc triển khai OpenSSL cập nhật.
 - Khóa RSA tự động ký 4096 bit. Khóa ngoài có thể được sử dụng thay thế.
 - NLA đến máy chủ.
- Giao thức SSH:
 - Dựa trên triển khai OpenSSL hiện đại, với các bản vá bảo mật và được biên soạn bởi WALLIX.
 - Dựa trên hầu hết các thuật toán mã hóa SSH tiên tiến.
 - Không hỗ trợ SSHv1.
 - Các thuật toán trao đổi khóa Diffie-Hellman tối thiểu 2048 bit.
- WALLIX Bastion hỗ trợ giao thức Kerberos mới nhất.
- WALLIX Bastion sử dụng khóa Master 256 bit để bảo vệ các dữ liệu nhạy cảm và tạo ra các khóa.

CHỐNG TÂN CÔNG TỪ CHỐI DỊCH VỤ

Vì WALLIX Bastion là portal cần thiết giữa mạng người dùng và mạng máy chủ, nó là mục tiêu được lựa chọn cho các cuộc tấn công DDOS để phá vỡ hệ thống. WALLIX Bastion dùng IPTABLE, chẳng hạn như giới hạn 50 kết nối mỗi giây hoặc 200 kết nối mỗi giây, để chống tấn công từ chối dịch vụ.

3.5. Giải pháp để xuất

Dựa trên nhu cầu của [CLIENT], chúng tôi đề xuất sử dụng giải pháp PAM Wallix Bastion bao gồm các mô đun sau:

- Session Manager: cho phép cung cấp tính năng kiểm toán đầy đủ và ghi lại các phiên người dùng
- Quản lý Password: cung cấp tính năng quản lý password tài nguyên đầy đủ

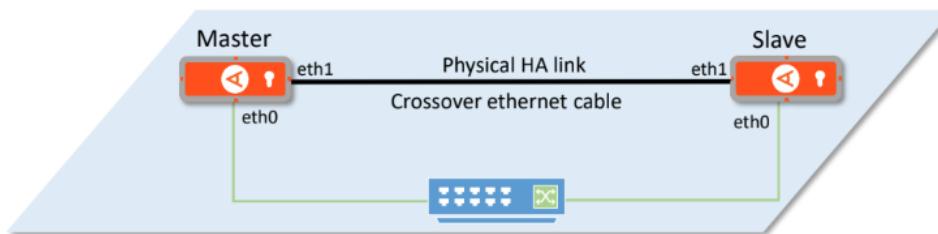
4. MÔ HÌNH TRIỂN KHAI ĐỀ XUẤT

4.1. Mục tiêu của triển khai PAM

- Tự động hóa quy trình quản lý tài khoản đặc quyền để quản lý hiệu quả việc bảo mật mật khẩu của tài khoản đặc quyền và cung cấp mật khẩu khi được yêu cầu 24x7
- Lưu trữ và quản lý mật khẩu an toàn để ngăn người dùng trái phép sử dụng các tài khoản đặc quyền
- Đảm bảo rằng mật khẩu duy nhất được phân bổ cho mỗi máy chủ / thiết bị / thiết bị chỉ cấp quyền truy cập khi cần và tự động thu hồi quyền truy cập khi hết hạn sử dụng
- Tránh sử dụng mật khẩu tĩnh và chia sẻ
- Đảm bảo rằng các tài khoản dịch vụ ứng dụng được phân bổ với mật khẩu duy nhất
- Tự động thay đổi mật khẩu của tài khoản dịch vụ ứng dụng

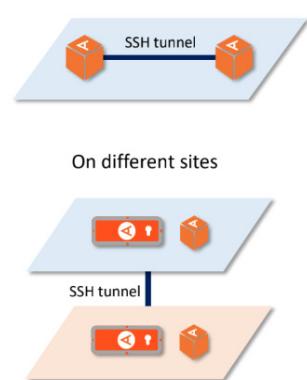
4.1. Mô hình triển khai

- Hỗ trợ chạy HA (Active/Passive)
 - Dùng Linux DRDB Technology (Mirroring)
 - Bastion Config
 - Connection Log
 - Session Record
 - Dùng chung 1 Virtual IP
 - Tự động chuyển đổi khi có lỗi

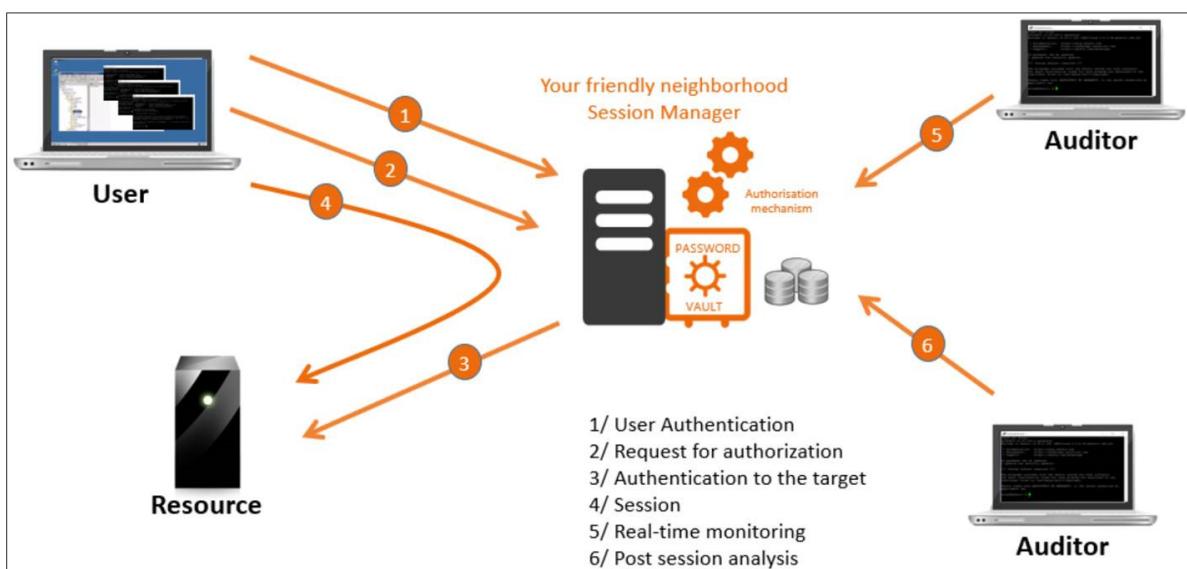


4

- Hỗ trợ mô hình Cluster / Replicate
 - Dữ liệu đồng bộ qua SSH Tunnel. Chỉ đồng bộ cấu hình / policy
 - Không dùng chung Virtual IP
 - Có thể kết hợp với Load balancer hoặc Wallix Access Manager
 - Có 2 mô hình
 - Hoặc Master/Slave (Nhiều Slave)
 - hoặc Master/Master (2 master, không có Slave)



4.2. Quy trình xử lý lưu lượng



1. Để cho phép người dùng đặc quyền (Kiểm toán, người dùng nội bộ, kỹ sư tích hợp, đối tác...) truy tập và bất kỳ thiết bị nào bên trong, những người dùng đặc quyền sẽ khởi tạo 1 kết nối SSH/RDP qua thiết bị PAM. Kết nối này sẽ được mã hóa.
2. Khi người dùng có đặc quyền truy cập thay đổi cấp độ hoặc nhiệm vụ công việc, họ cần được phê duyệt cấp cho mật khẩu đặc quyền mới, mẫu phê duyệt sẽ được gửi người dùng cần cấp đặc quyền để điền yêu cầu phê duyệt.
3. Khi người dùng đặc quyền được xác thực, kết nối SSH (SSH/Telnet/RLOGIN) hoặc RDP từ PAM tới thiết bị đích sẽ được thiết lập để mở truy cập cho người dùng đặc quyền đến các thiết bị cần quản trị. Kết nối này cũng sẽ được yêu cầu tuân thủ các chuẩn mã hóa cao nhất có thể.
4. PAM bắt đầu giám sát các phiên sau khi người dùng được xác thực. Trong trường hợp nếu hành vi của người dùng được xác thực kích hoạt các hành động bị cấm đã được tích hợp trong hệ thống, phiên ghi sẽ dừng lại và kích hoạt báo cáo gửi người quản trị cấp cao – “Supervisor”.
5. Khi người quản trị Supervisor/ Auditor muốn kiểm tra thông tin thống kê về phiên người dùng, họ có thể truy cập vào PAM để xem các phiên “LIVE” về những người dùng được cấp quyền về hành động của họ bao gồm các thông tin: “Cái gì”, “Ở đâu”, “khi nào”, “Tại sao” theo thời gian thực.
6. Người kiểm toán “Auditor” có thể gửi các thông tin kiểm toán phiên đảm bảo rằng các phiên này đã được hoàn thiện mà không có vấn đề gì.

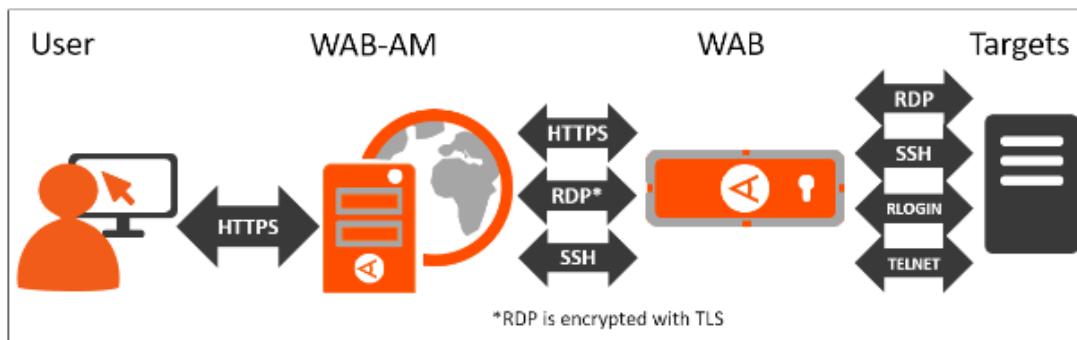
4.3. Phương án triển khai mở rộng

Nếu [CLIENT] có ý định mở rộng nền tảng Cloud trong lai gần, công nghệ của WALLIX cho phép mở rộng và tích hợp với bất kỳ môi trường ảo nào bao gồm cả nền tảng đám mây. Ngoài ra, Wallix có tùy chọn mô đun BASTION Access Manager cho phép [CLIENT] triển khai với dịch vụ multi-tenancy, khi đó [CLIENT] nêu có 1 bộ phân riêng cũng được giám sát bởi thiết bị WALLIX. Theo cách này, 1 thiết bị WALLIX tập trung cho phép quản lý, truy vết, kiểm toán, và ghi lại hoạt động từ các thiết bị đích nằm tại nhiều công ty con khác nhau.

Bastion Access Manager cung cấp kết nối từ nhiều web browser đến nhiều thiết bị đích khác nhau sau khi họ được xác thực. Các thiết bị đích được truy cập thông qua hệ thống WALLIX Bastion. Kết nối này được thực hiện qua giao thức html5 mà không cần cài thêm plugin cho browser.

Bastion Access Manager cho phép người dùng với đặc quyền truy cập xem password được cấp trong trình duyệt truy cập quản trị và/ hoặc cõi chúng ra ngoài.

Bastion Access Manager hỗ trợ triển khai dịch vụ multi-tenancy và những người dùng có đặc quyền có thể truy cập vào các thiết bị đích hoặc các ứng dụng đích mà không gây xáo trộn/ ngắt quãng các kết nối vì vậy Bộ tư lệnh [CLIENT] có thể triển khai trên bất kỳ dịch vụ multi-tenancy nào trên nền tảng cloud.



Bastion Access Manager thường được thiết lập trong môi trường DMZ với các API truy cập vào WALLIX Bastion nhằm bảo mật các truy cập tới Bastion, cho phép người dùng kết nối qua Firewall tới mô đun Bastion Access manager thông qua HTTPS/ HTML5 thay vì sử dụng VPN.

Với tính năng Clustering của Bastion, BASTION ACCESS MANAGER cho phép triển khai cân bằng tải, đảm bảo tính sẵn sàng cao nhất cho kết nối và trải nghiệm của người dùng. Tính năng Clustering cũng đảm bảo tính HA và cải tiến tốt hơn quá trình recovery. Người quản trị và người dùng có thể kết nối từ xa qua hệ thống hỗ trợ HTTPS/ HTML5 bao gồm các máy tính bảng kết nối qua 4G, giúp giảm nhu cầu tìm kiếm các điểm truy cập wifi khi kết nối bằng máy tính xách tay.

Với mô đun Bastion Access Manager, người dùng có thể dễ dàng kiểm tra loại thiết bị hoặc ứng dụng mà họ đã kết nối tới sau khi xác thực thành công.

5. TÍNH NĂNG VÀ LỢI ÍCH CỦA GIẢI PHÁP

WAB được phát triển nhằm giúp những giám đốc, trưởng phòng IT quản lý hạ tầng IT một cách hiệu quả hơn (Máy chủ, thiết bị mạng, thiết bị bảo mật...). Giải pháp này được thiết kế đáp ứng các yêu cầu về kiểm soát truy cập, tính năng truy vết cần thiết cho người quản lý hạ tầng mạng.

WAB bao gồm các danh sách truy cập (access list – ACL) và tính năng truy vết. Nó là bộ đệm bảo mật giữa những người dùng được cấp quyền và hệ thống IT mà họ muốn đăng nhập vào quản trị, bằng cách

- Kiểm tra chi tiết thông tin xác thực người dùng cung cấp
- Kiểm tra quyền của họ đối với thiết bị họ muốn truy cập
- Quản lý các tài khoản thực của thiết bị/ ứng dụng

Hệ thống cũng cho phép người dùng tự động đăng nhập vào các thiết bị với tính năng nân cao cấp độ bảo mật bằng việc ẩn đi những thông tin xác thực thật của máy chủ, thiết bị.

Các giao thức hệ thống hiện hỗ trợ:

- SSH
- Telnet, Rlogin
- RDP và VNC

WAB cung cấp giao diện người dùng Web-based (viết tắt là “GUI”) tương thích với Internet

Explorer, Chrome và Firefox để giám sát mọi hành vi và phiên kết nối người dùng.

5.1. Quản lý truy cập người dùng

WAB phát triển nâng cao tính năng quản lý quyền truy cập dựa trên tính năng ACL để xác định ai, cái gì, khi nào và giao thức nào được người dùng xác thực sử dụng.

Những ACL này bao gồm những đối tượng sau:

- Người dùng: người dùng thực của WAB được xác thực từ thư mục người dùng bên trong và bên ngoài thiết bị WAB
- Nhóm người dùng: tập hợp những người dùng: user group
- Thiết bị: Các thiết bị vật lý và ảo hóa được nhận yêu cầu truy cập từ WAB
- Các tài khoản thực: Các tài khoản được khai báo trên thiết bị hoặc ứng dụng
- Các nhóm tài khoản thực: target account groups
- Các ứng dụng: Bất kể ứng dụng, dịch nào chạy trên thiết bị hoặc nhóm thiết bị

Trong WAB, việc xác thực phải được thiết lập để đồng ý 1 người dùng truy cập tới tài khoản thực. Những xác thực được khai báo giữa 1 nhóm người dùng và 1 nhóm tài khoản thực (nghĩa là mỗi tài khoản thực phải thuộc 1 nhóm tài khoản thực “arget account group”, và mỗi người dùng phải thuộc 1 nhóm người dùng “user group”)

Việc xác thực này cho phép những người dùng ở nhóm X truy cập tới các tài khoản thực ở nhóm Y, thông qua giao thức: A hoặc B, hoặc C.

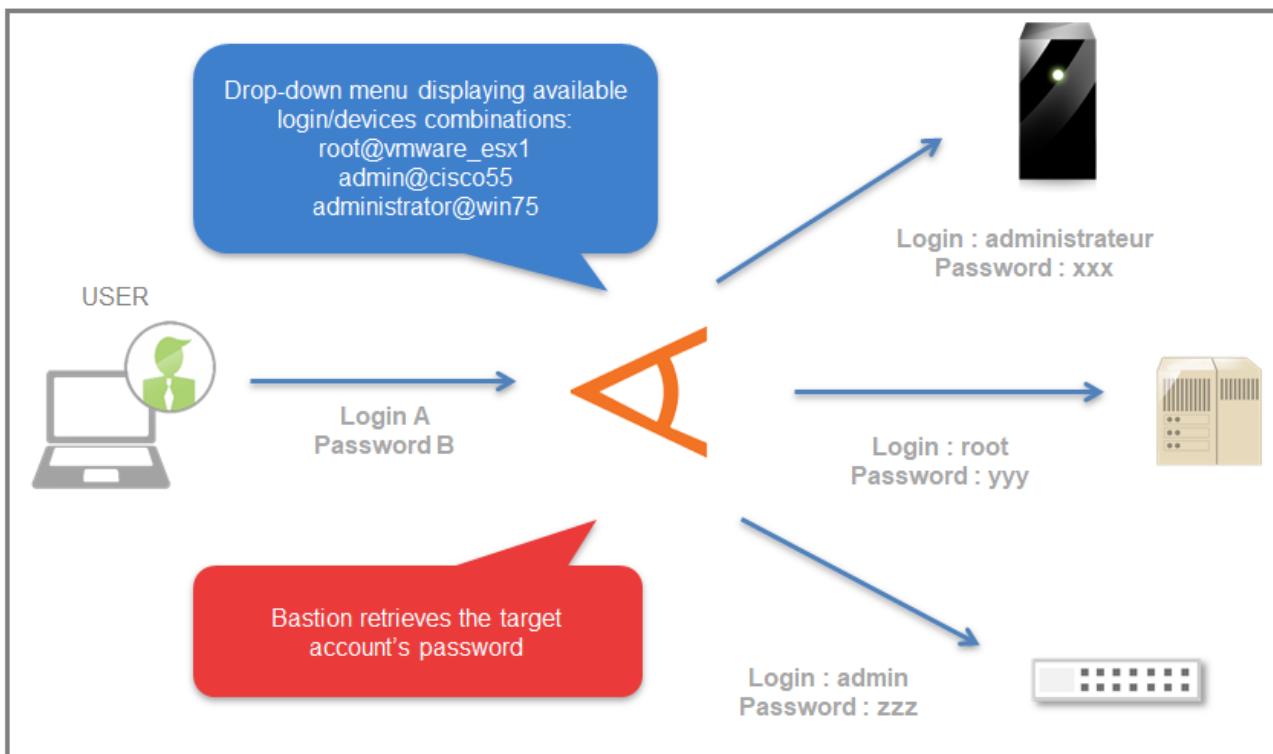
Những thành phần khác được thêm vào các thực thể này, cho phép người quản trị định nghĩa là:

- Khung thời gian kết nối
- Cấp độ quan trọng của truy cập tới các tài khoản đích



- Có cần phải ghi lại phiên kết nối người dùng hay không
- Loại thủ tục xác thực người dùng.

Trong hệ thống Bastion: Mật khẩu gốc của tài khoản quản lý/thiết bị được lưu trong Bastion (xem mode SSO), vì vậy người dùng không cần phải biết mật khẩu gốc này. Hệ thống sẽ cung cấp cho người dùng 1 tài khoản tạm thời để truy cập vào quản trị thiết bị.



Bastion sử dụng chế độ “Match Accounts” để xác thực người dùng kết nối đến thiết bị đích khi đăng nhập qua hệ thống của Bastion (xem hình sau)



Ghi chú: mỗi xác thực người dùng được gắn với 1 khe thời gian (là thời gian bắt đầu và kết thúc 1 kết nối) cũng như tùy chọn ngắt kết nối khi kết thúc thời gian đó

5.2. Cơ chế xác thực mạnh mẽ

WAB sử dụng cơ chế xác thực mạnh mẽ, cho phép hệ thống kết nối xác thực đến các máy chủ xác thực Radius bên ngoài. Nó được sử dụng để xác thực qua giao thức OTP mạnh mẽ (RSA, Secur ID hoặc tương tự)

WALLIX sử dụng chứng chỉ PKI bao gồm các Keynectis OpenTrust để xác thực người dùng qua các chứng chỉ điện tử X509V3.

5.3. Quản lý tài khoản người dùng đơn giản, thuận tiện.

Sử dụng giải pháp Bastion cho phép người quản trị sử dụng trang “Account” – tài khoản người dùng để:

- Liệt kê, kiểm soát danh sách các tài khoản người dùng, họ có thể lọc theo tài khoản nội bộ hay tài khoản tên miền từ các domain Active Directory và LDAP.
- Tạo/ sửa/ xóa 1 tài khoản
- Định nghĩa những người dùng có quyền khôi phục thông tin xác thực: những người này sẽ nhận được email về mật khẩu mới mỗi lần khôi phục tài khoản truy cập – tính năng này sử dụng cho những nhân viên trong city mỗi khi họ thường xuyên có yêu cầu truy cập vào hệ thống nào đó.
- Xem thông tin chi tiết về quyền và ứng dụng, thiết bị truy cập và thông tin của từng tài khoản.
- Mở khóa cho tài khoản người dùng chỉ bằng 1 click
- Nhập thông tin về người dùng từ file.csv

Người quản trị có thể lọc thông tin hiển thị về các tài khoản cần tìm kiếm thông tin liên quan tới các dữ liệu của các tài khoản quản lý.

| User name | Display name | Profile | Authentication | Groups | Account locked/expired | Last connection |
|---------------|-------------------------|----------------------|----------------|--|------------------------|---------------------|
| admin | WAB Super Administrator | WAB_administrator | local | Group1, UserGroup1, UserGroup2, Group2 | | 2016-09-28 10:38:54 |
| Doe | John Doe | approver | local | Group1, UserGroup1, UserGroup2, Group2 | | -- |
| Martin | Lucas Martin | user | local | Group1, Group2 | | 2016-09-14 16:07:14 |
| userTest01 | UserTest01 | profiletest | local | Group1, Group2 | | 2015-12-23 09:36:54 |
| userTest03 | UserTest03 | approver | local | Group1, UserGroup1, UserGroup2, Group2 | | -- |
| userTest04 | UserTest04 | profiletest | local | Group1, UserGroup2, Group2 | | -- |
| userTest02 | UserTest02 | WAB_administrator | local | UserGroup1, UserGroup2 | | -- |
| UserTraining1 | User Training 1 | WAB_administrator | local | TrainingGroup1 | | 2016-04-20 15:28:59 |
| UserTraining2 | User Training 2 | user | local | TrainingGroup1 | | -- |
| UserTraining3 | User Training 3 | system_administrator | local | TrainingGroup1 | | -- |

Màn hình giám sát người dùng của người quản trị

Các quản trị viên được xác định trong cơ sở dữ liệu nội bộ của Bastion hoặc thư mục LDAP / LDAPS bên ngoài, Active Directory hoặc Radius.

Lưu ý: có thể sử dụng kết hợp nhiều loại nhận dạng người dùng.

Nếu cơ sở dữ liệu nội bộ của Bastion (LDAP) được sử dụng để nhận dạng người dùng, Bastion áp dụng chính sách bảo mật được xác định trước cho mật khẩu người dùng.

Nhận dạng người dùng cũng có thể ủy quyền cho một thư mục Active Directory hoặc LDAP bên ngoài. Trong trường hợp này, bạn phải chỉ định thư mục xác thực chính bên ngoài của Bastion và ánh xạ các nhóm người dùng AD / LDAP sang các nhóm người dùng Bastion.



The screenshot shows the WALLIX Bastion Configuration interface. The left sidebar includes links for My authorizations, Audit, Users, Targets, Authorizations, Session management, Password management, Configuration (which is selected), and System.

The main content area is titled "Add LDAP/AD domain". It contains the following fields:

- Bastion domain name ***: Acme
- Description**: (empty text area)
- Default domain**: (checkbox) If you check this option, this domain will replace "bizsecure.local" as default LDAP/AD domain
- LDAP/AD domain name ***: (empty text area)
- Directory**: (checkbox) (Available Directories: Select all; Selected Directories: Delete all)
- Secondary authentication**: (Available Secondary Authentications: InWebo; Selected Secondary Authentications: Select all; Delete all)
- User attributes**: (Group attribute, Display name attribute, Email attribute, Default email domain *, Language attribute, Default language *: English)
- X509 options**: (X509 authentication, Matching condition, Search filter, Domain name to match SAN Email)
- LDAP authentication mapping**: (User group *: Application-Admin; Profile *: user; LDAP group *: Default group for users without group in this domain; another row: Application-Admin; user)

Nếu người dùng không khai báo trong Bastion khi họ có găng kết nối, Bastion sẽ thám vấn một thư mục bên ngoài được xác định trước để tìm ra nhóm AD / LDAP nào mà người dùng thuộc về tất cả các đăng nhập / thiết bị được ủy quyền của họ kết hợp có thể được lấy.

Lưu ý: hai cơ chế có thể sử dụng cùng nhau, với một số người dùng được khai báo trực tiếp trong Bastion trong khi chi tiết xác thực của những người khác được lấy từ một thư mục bên ngoài.

Khi kết nối SSH được sử dụng, người dùng có thể được xác thực bằng phương thức xác thực hai yếu tố SSH. Trong trường hợp này, họ phải tải lên các khóa công khai SSH của mình lên Bastion để sau đó chúng có thể được xác thực bằng các khóa riêng SSH của họ.



Bastion cũng có thể được sử dụng khi dữ liệu xác thực được truyền bằng cách sử dụng tác nhân SSH; trong trường hợp này, Bastion gửi khóa riêng của người dùng đến thiết bị đích.

5.4. Quản lý “kho” lưu trữ thông tin tài khoản thực, thông tin thiết bị thuận tiện

Sử dụng giải pháp Bastion cho phép người quản trị sử dụng Trang “resource” – “Tài nguyên” để tạo và quản lý “Domain” (tên miền), các thiết bị, các ứng dụng và các tài khoản thực của thiết bị, ứng dụng

Ghi chú: Domain là nhóm các tài khoản sử dụng để xác thực truy cập vào thiết bị/ ứng dụng. Tài khoản xác thực thiết bị gọi là tài khoản target.

Bao gồm các tính năng chính:

- Liệt kê danh sách Domain/ thiết bị/ ứng dụng
- Tạo/Hiệu chỉnh/ xóa thông tin Domain/ Thiết bị/ Ứng dụng
- Nhập thông tin từ file .csv (file này có thể được xuất ra từ cơ sở dữ liệu của thiết bị Bastion khác)
- Thiết lập tính năng tự động thay đổi mật khẩu thực định kỳ theo chính sách thay đổi mật khẩu mà người quản trị đặt ra.

The screenshot shows the WAB (Web Application Backend) interface. On the left, there's a sidebar with various menu items like My Preferences, My Authorizations, Audit, Users, Resources, Domains, Devices, Applications, Accounts, Clusters, Groups, Checkout Policies, Password Management, Session Management, Authorizations, Configuration, System, and Import/Export. The 'Devices' item is currently selected. The main content area has a title 'Create a device'. It contains several input fields: 'Name*' (with a red asterisk indicating it's required), 'Alias', 'Device host*' (with a note about supported syntax: xxxxx (IP), xxxxx/w (subnet) or hostname), 'Description', and 'Local domains' (with a 'Name*' field and a plus sign icon). Below these is a 'Services' section with checkboxes for VNC, RDP, RLOGIN, TELNET, and SSH. At the bottom right are 'Cancel' and 'Apply' buttons.

Trang Resource khi tạo mới thiết bị

5.5. Chế độ SSO mode

WAB cho phép người quản trị cấp tính năng SSO (đăng nhập 1 lần) để đăng nhập vào thiết bị WAB, với các thông tin về tài khoản và thiết bị người dùng đã đăng ký trước đó, họ sẽ được kết nối trực tiếp tới các thiết bị mà họ đăng ký để truy cập vào quản trị trước đó mà không cần xác thực lại.

WAB cung cấp tính năng SSO này cho phép tất cả người dùng kết nối tới các thiết bị đã được đăng ký và xác thực để quản trị với mật khẩu riêng của họ, mà không cần khai báo thêm mật khẩu gốc trên thiết bị

5.6. Traceability – tính năng truy vết

Toàn bộ các kết nối của người dùng đều được hệ thống lưu log lại

| User | Target | Target host/IP | SRC/DST protocol | Start time | End time | Duration | Size | Res |
|----------------------|-----------------------------------|----------------|-----------------------|---------------------|---------------------|----------|----------|-----|
| robinhood@10.0.0.52 | administrator@local@W2k16-01:3389 | 10.0.0.41 | RDP/RDP | 2021-03-12 10:13:33 | 2021-03-12 10:14:41 | 00:01:08 | -- | ✓ |
| robinhood@10.0.0.52 | administrator@local@W2k16-01:3389 | 10.0.0.41 | RDP/RDP | 2021-03-12 10:12:30 | 2021-03-12 10:12:37 | 00:00:07 | -- | ✓ |
| robinhood@10.0.0.52 | administrator@local@W2k16-01:3389 | 10.0.0.41 | RDP/RDP | 2021-03-12 08:47:57 | 2021-03-12 08:48:02 | 00:00:05 | -- | ✓ |
| robinhood@10.0.0.52 | administrator@local@W2k16-01:3389 | 10.0.0.41 | RDP/RDP | 2021-03-12 08:47:14 | 2021-03-12 08:47:16 | 00:00:02 | -- | ✓ |
| robinhood@10.0.0.64 | administrator@local@W2k16-01:3389 | 10.0.0.41 | RDP/RDP | 2020-11-13 09:48:47 | 2020-11-13 10:02:39 | 00:13:52 | 827.3 KB | ✓ |
| robinhood@10.0.0.64 | administrator@local@W2k16-01:3389 | 10.0.0.41 | RDP/RDP | 2020-11-13 09:16:47 | 2020-11-13 09:32:49 | 00:16:02 | 46.6 KB | ✓ |
| robinhood@10.0.0.115 | admin@local@Ubuntu2004:22 | 10.0.0.80 | SSH/SSH_SHELL_SESSION | 2020-11-10 11:11:18 | 2020-11-10 11:12:42 | 00:01:24 | 3.0 KB | ✗ |
| robinhood@10.0.0.115 | admin@local@Ubuntu2004:22 | 10.0.0.80 | SSH/SSH_SHELL_SESSION | 2020-11-10 11:09:39 | 2020-11-10 11:11:07 | 00:01:28 | 1.7 KB | ✗ |
| robinhood@10.0.0.115 | robinhood@Firefox | 10.0.0.41 | APP/RDP | 2020-11-10 11:07:23 | 2020-11-10 11:08:45 | 00:01:22 | 7.3 MB | ✓ |
| robinhood@10.0.0.115 | administrator@local@W2k16-01:3389 | 10.0.0.41 | RDP/RDP | 2020-11-10 11:01:39 | 2020-11-10 11:03:02 | 00:01:23 | 95.1 KB | ✓ |

✓ : Kết nối bình thường

✗ : Kết nối đóng bởi người quản trị WAB

❗ : Phiên kết nối không mở, bị lỗi (Ví dụ trường hợp thiết bị quản trị không tìm thấy)

Toàn bộ các kết nối được ghi lại và cho phép xem lại (ở mục Reporting và Audit) và cho phép xuất ra các định dạng chung để xem ở bên ngoài thiết bị WAB.

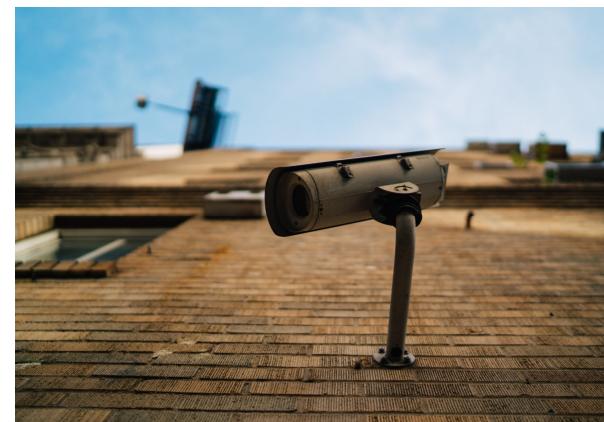
Ghi chú:

- Tính năng này không chỉ ghi phiên kết nối người dùng, mà còn lưu lại tất cả các hành động của người quản trị trên thiết bị WAB.
- Tất cả các phiên mà người dùng đang mở đều được giám sát trực tiếp và người có thể ngắt phiên kết nối này khi cần thiết.

5.7. Vai trò của mô đun Session Management

Kiểm soát và giám sát mọi truy cập của người dùng được phân quyền

- ✓ Trình quản lý phiên cho phép người quản trị hệ thống theo dõi mọi hành động trong quá trình người dùng được phân quyền thực hiện trong hệ thống, bao gồm cả tính năng giám sát và xem lại chúng khi cần thiết.
- ✓ Quản trị viên có quyền hạn chế quyền truy cập của người dùng khi thấy có những hành vi bất thường như: tạo mật khẩu quản trị trái phép, hoặc tự động xóa cấu hình quan trọng...
- ✓ Trình quản lý phiên cho phép tích hợp vào các công cụ bảo mật khác như SIEM, SOAR và



IDS để xác định và ngăn chặn các cuộc tấn công tiềm ẩn trước khi chúng xảy ra.

5.7.1 Kiểm soát, giám sát và gửi cảnh báo theo thời gian thực

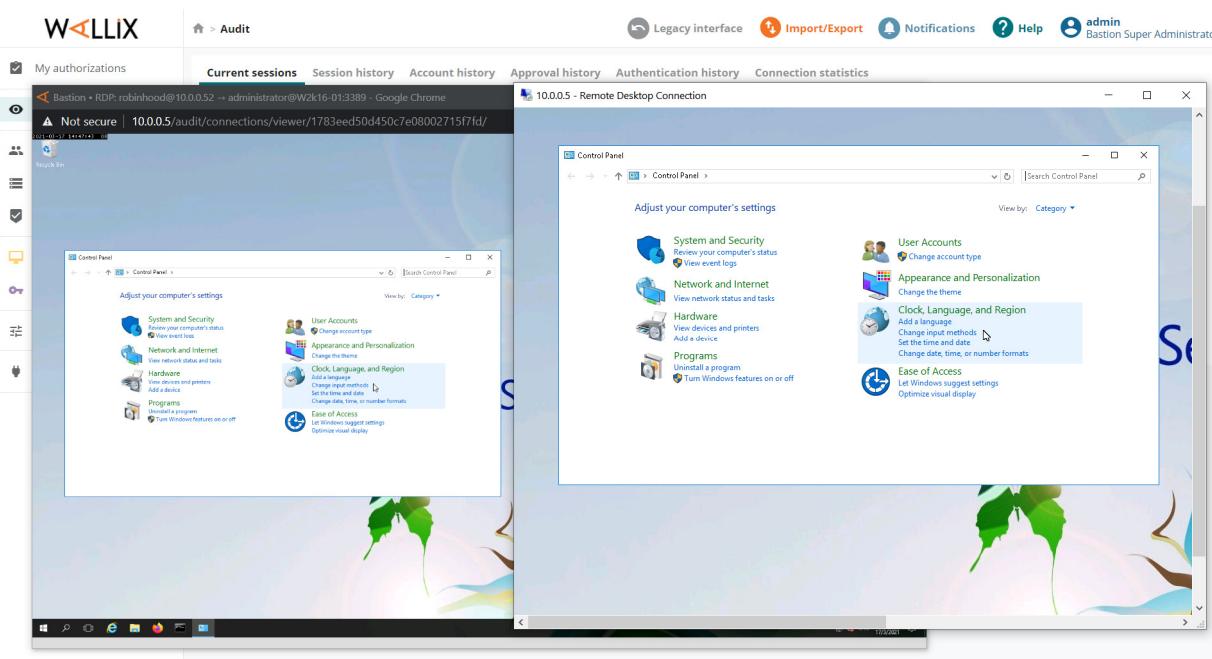
Ngoài việc cho phép truy vết lại các kết nối trong quá khứ, Wallix Bastion cho phép giám sát theo thời gian thực

- Nâng cao khả năng ứng phó với những “sự cố” bằng việc kết hợp giữa công nghệ giảm thiểu rủi ro với sự kiểm soát chủ động của người quản lý.
- Tính năng này cho phép từ màn hình giám sát thông qua thiết bị trung tâm của Wallix Bastion.
- người quản trị theo dõi hành động của người dùng sau khi họ đăng nhập thành công vào cấu hình thiết bị, máy chủ hay sử dụng các ứng dụng
- Với những hành động hoặc thao tác cấu hình lệnh không tuân thủ theo chính sách bảo mật, người quản trị sẽ chủ động ngắt kết nối khi cần thiết.

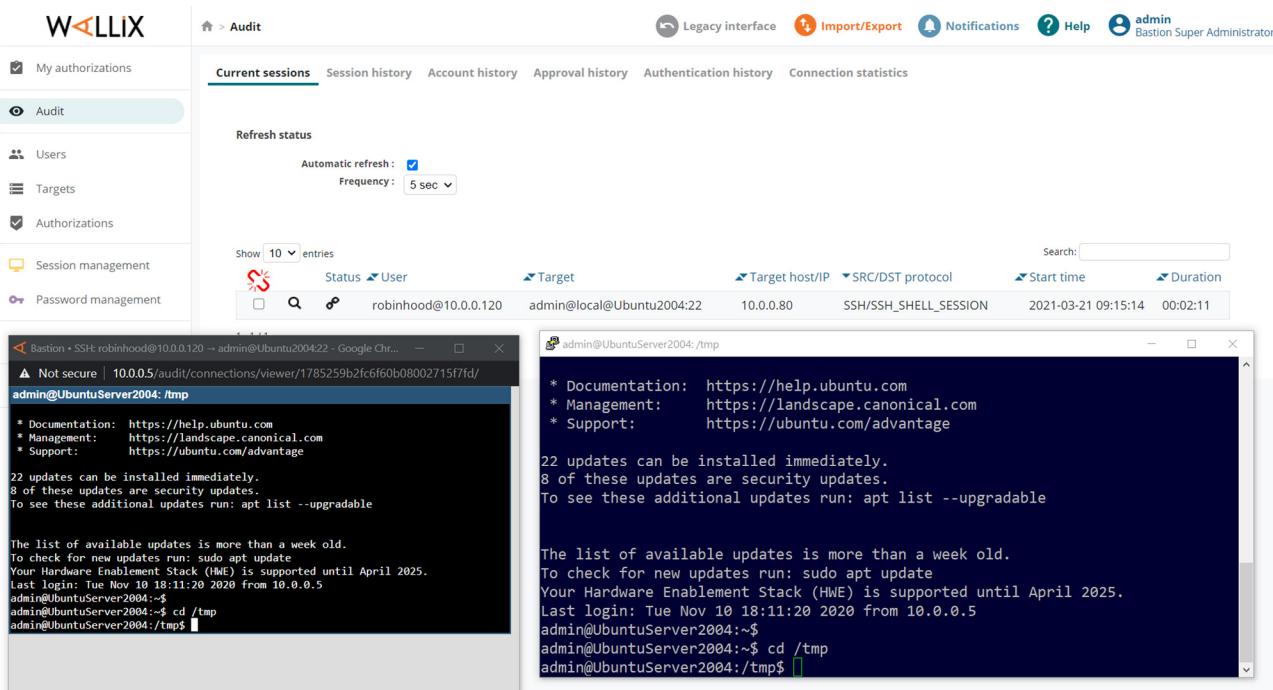
| Status | User | Target | Target host/IP | SRC/DST protocol | Start time | Duration |
|--------|----------------------|-----------------------------------|----------------|-----------------------|---------------------|----------|
| SSH | robinhood@10.0.0.120 | admin@local@Ubuntu2004:22 | 10.0.0.80 | SSH/SSH_SHELL_SESSION | 2021-03-21 09:15:14 | 00:04:20 |
| SSH | robinhood@10.0.0.120 | administrator@local@W2k16-01:3389 | 10.0.0.41 | RDP/RDP | 2021-03-21 09:19:14 | 00:00:20 |

- Thông qua giao diện này, các user có thẩm quyền có thể
 - o Xem trực tiếp những gì đang trực tiếp diễn ra
 - o Ngắt kết nối nếu muốn (Kết nối cũng có thể ngắt tự động nếu người dùng có hành vi vi phạm các chính sách đã được thiết lập như gõ lệnh không cho phép, có tiến trình không được phép chạy mở lên..)
 - o Nhảy vào chung cùng 1 phiên (giống như dùng tính năng Ultraviewer hay teamviewer) – Xem thêm về tính năng Session Sharing

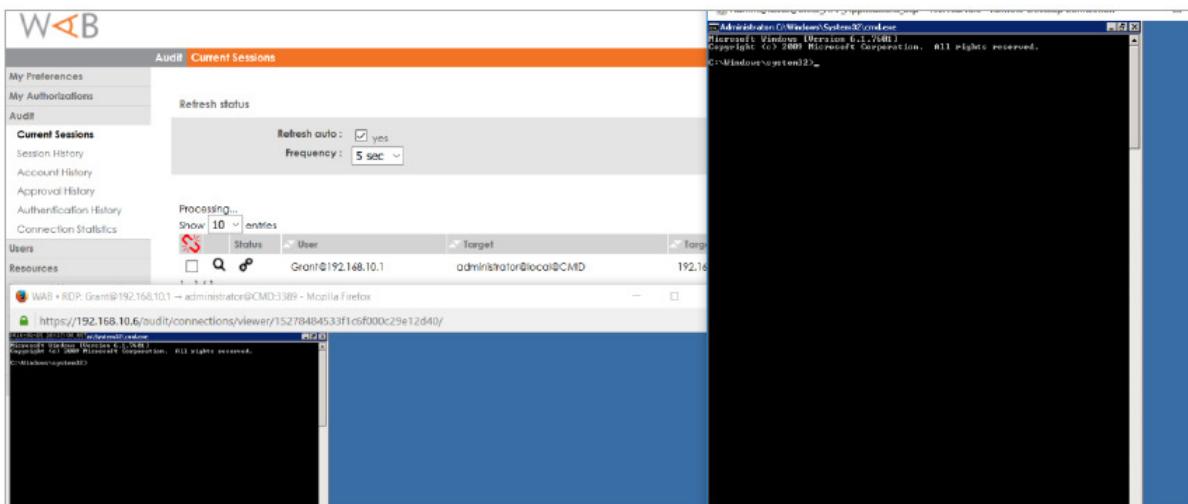
+ Màn hình giám sát khi người dùng sử dụng giao thức RDP truy cập vào máy chủ



+ hay các phiên truy cập SSH được giám sát từ xa



+ hoặc ứng dụng của người dùng được giám sát trên màn hình quản lý



Đồng thời hệ thống cho phép người quản trị chủ động ngắt kết nối khi người dùng truy cập vi phạm quy tắc về bảo mật mạng. Đồng thời hệ thống cũng gửi cho người dùng truy cập được biết về việc họ đã bị ngắt kết nối cùng lý do đi kèm

```

2 | test@debian32:SSH_22
3 | root@debian64:SSH_22
4 | qa\administrateur@win2k3:TELNET_23
5 | qa\administrateur@win2k3dc:TELNET_23
6 | qa\administrateur@winxp:TELNET_23
Connect to (ctrl-D to quit): 1

Welcome on Wellix AdminBastion

Your actions could be recorded and stored in electronic format.
Please contact your AdminBastion administrator for more precisions.

Warning: This connection will be closed at 2099-12-30 23:59:59
Linux debian32.qa.ifr.lan 2.6.26-2-686 #1 SMP Thu Nov 25 01:53:57 UTC 2010 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar 28 04:16:42 2012 from 10.10.47.187
debian32:~# echo $0
-bash
debian32:~#
Connection closed by your administrator

```

5.7.2 Hỗ trợ kiểm soát truy cập đối với các giao thức RDP và SSH từ máy người dùng

Giúp ngăn chặn các cuộc tấn công từ trong mạng, vấn đề leo thang tài khoản đặc quyền, và giảm thiểu các vấn đề phát sinh từ công cụ của bên thứ 3.

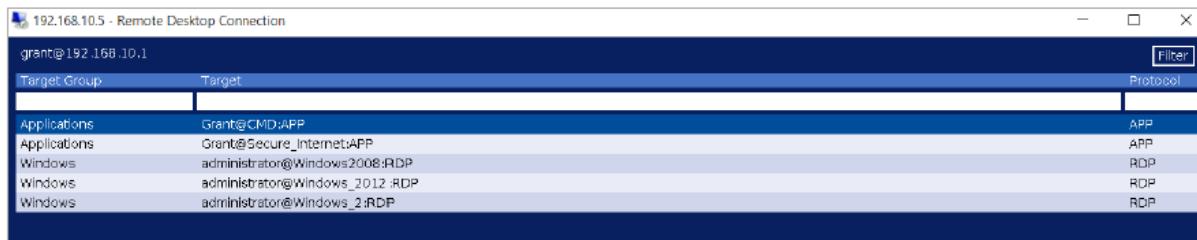


Để kết nối vào các hệ thống đầu cuối, người dùng sẽ phải dùng 1 trong 2 phương thức

- Hoặc SSH (cho các giao thức SSH/Telnet/Rlogin/Raw TCP)
- Hoặc RDP (cho RDP/VNC)

Trong cả 2 phương thức này WAB hỗ trợ người dùng

- Kết nối trực tiếp vào hệ thống cần quản trị
- Hoặc kết nối vào Wallix Bastion trước. Sau khi xác thực người dùng bằng tài khoản trên PAM, hệ thống sẽ hiển thị các hệ thống đầu cuối mà người dùng được phép truy cập vào



The screenshot shows a terminal window titled "192.168.10.5 - PuTTY". The session log contains the following text:

```
login as: grant
Using keyboard-interactive authentication.
grant's password:
| ID | Site (page 1/1)      | Group
|---|-----|-----|
| 0 | admin@Linux1:SSH_2 | Linux
| 1 | admin@Linux2:SSH    | Linux
Enter h for help, ctrl-D to quit
>
Press 'n' for next page
Press 'p' for previous page
Press 'f <pattern>' to filter targets list
Press 'f' to remove a filter
Press 'q' to quit
Press '<site_id>' to connect to a site
Enter h for help, ctrl-D to quit
> [redacted]
```

5.7.2.4. Kiểm soát phiên truy cập qua SSH

Các phiên SSH / telnet / rlogin được giám sát theo thời gian thực cũng như cho xem lại

The screenshot displays the WAB application interface. On the left, a sidebar lists various audit categories: My Preferences, My Authorizations, Audit, Current Sessions, Session History, Account History, Approval History, Authentication History, Connection Statistics, Users, Resources, Password Management, Session Management, Authorizations, Configuration, System, and Import/Export. The 'Session History' tab is currently selected.

The main content area is divided into three sections:

- Session info:** Displays detailed information about a specific session. The session details are as follows:
 - User name: Grant@192.168.10.1
 - Target: admin@local@Ubuntu:22
 - Target host/IP: 192.168.10.128
 - SRC/DST Protocol: SSH/SSH_SHELL_SESSION
 - start time: 2014-01-25 12:38:34
 - End time: 2014-01-25 12:40:43
 - Duration: 0:02:09
 - Result: Killed by admin
 - Description: --
- Viewer:** A video player interface showing a play button icon. Below the video player, the text "PLAYTERM.DRS" is visible.
- Transcription:** A text box containing the terminal session transcript:

```
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-34-generic #53-Ubuntu)
 * Documentation: https://help.ubuntu.com/
Last login: Mon Jan 26 10:08:14 2015 from 192.168.10.6
admin@grant-virtual-machine:~$
```

Tệp văn bản chứa toàn bộ phiên SSH có thể được mở trực tiếp bằng trình xử lý văn bản như MS Word.

Transcription

```
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-52-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

244 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue Nov 10 18:09:41 2020 from 10.0.0.5
admin@UbuntuServer2004:~$ 
admin@UbuntuServer2004:~$ cd /tmp
admin@UbuntuServer2004:/tmp$ ls
systemd-private-94c5561f4ac8428c90f79a9842023259-colord.service-zH04tf
systemd-private-94c5561f4ac8428c90f79a9842023259-ModemManager.service-cB6SNg
systemd-private-94c5561f4ac8428c90f79a9842023259-switcheroo-control.service-grTZ
systemd-private-94c5561f4ac8428c90f79a9842023259-switcheroo-control.service-grTZEH
systemd-private-94c5561f4ac8428c90f79a9842023259-systemd-logind.service-vWvRkg
systemd-private-94c5561f4ac8428c90f79a9842023259-systemd-resolved.service-PyKwkf
systemd-private-94c5561f4ac8428c90f79a9842023259-systemd-timesyncd.service-w1m9b
systemd-private-94c5561f4ac8428c90f79a9842023259-systemd-timesyncd.service-w1m9bf
systemd-private-94c5561f4ac8428c90f79a9842023259-upower.service-ACEPki
tracker-extract-files.1001
tracker-extract-files.125
VMwareDnD
admin@UbuntuServer2004:/tmp$ hello

Command 'hello' not found, but can be installed with:

sudo snap install hello          # version 2.10, or
sudo apt install hello           # version 2.10-2ubuntu2
sudo apt install hello-traditional # version 2.10-5

See 'snap info hello' for additional versions.
```

Session metadata

```
2020-11-10 11:11:18 type="SESSION_ESTABLISHED_SUCCESSFULLY"
2020-11-10 11:11:42 type="KBD_INPUT" data="cd /tmp"
2020-11-10 11:11:43 type="KBD_INPUT" data="ls"
2020-11-10 11:12:28 type="KBD_INPUT" data="hello"
2020-11-10 11:12:42 type="SESSION_DISCONNECTED" duration="0:01:24"
```

5.7.2.5. Kiểm soát phiên truy cập qua RDP và xRDP

Wallix Bastion cho phép bạn xem bản ghi video của các phiên ứng dụng RDP, VNC và máy khách/máy chủ, cũng như nội dung phiên.



The screenshot shows the Wallix Bastion web interface. On the left, there's a sidebar with navigation links like 'My Preferences', 'My Authorizations', 'Audit', 'Current Sessions', 'Session History' (which is selected), 'Account History', 'Approval History', 'Authentication History', 'Connection statistics', 'Users', 'Resources', 'Password Management', 'Session management', 'Authorizations', 'Configuration', 'System', and 'Import/Export'. The main area has tabs for 'Audit' and 'Session history'. Under 'Session history', it says 'Session info' and lists details: User name: CROM@192.168.10.1; Target: administrator@local@DC01; SSO; Target host IP: 192.168.10.151; SNC/DST Protocol: RDP/RDP; Start time: 2016-01-25 12:46:44; End time: 2016-01-25 12:47:07; Duration: 00:00:23; Result: Success; Description: -. Below this is an 'RDP Viewer' section with a large black video frame containing a play button icon. At the bottom of the frame is a checkbox labeled 'Continuous playback' with a checked mark.

Nhờ tính năng Session Probe và tính năng OCR(Optical Character Recognition), Wallix Bastion thu thập Metadata và gắn liền với từng phần đoạn video giúp cho việc tìm kiếm, truy vết hiệu quả hơn.

- Các process được mở và tắt
- Tiêu đề của các cửa sổ đang hoạt động
- Bàn phím (key log)
- Các nút được nhấp
- Nội dung Clipboard sao chép qua lại
- Sự kiện Kerberos
- V.v.

The screenshot shows the Wallix Bastion interface. At the top, it says "Screenshots list" and displays four thumbnail images of RDP sessions. Below this, there is a "Session data" section with a download icon. A table below lists session details:

| Index | Date Time | Content |
|-------|------------------------|-------------------------|
| 1 | 2016-01-25 12:46:42 | Beginning |
| 2 | 2016-01-25 12:46:49 | All Control Panel Items |
| 3 | 2016-01-25 12:46:52 | Folder Options |
| 4 | 2016-01-25 12:46:55 | All Control Panel Items |
| 5 | 2016-01-25 12:47:00 | Sound |

Tính năng OCR

Tính năng OCR sẽ nhận dạng tiêu đề các cửa sổ (window caption), Nội dung các nút nhấn, .v.v cho phép thu thập thông tin về ứng dụng đang chạy và tên của tệp mà ứng dụng được sử dụng.

Lưu ý: tính năng OCR cũng phát hiện điều hướng trong cấu trúc cây hoặc đĩa mạng.

Tất cả dữ liệu Metadata có thể được đẩy về hệ thống SIEM, SOAR, Syslog, v.v. theo thời gian thực giúp hệ thống có thể phát hiện và ngăn chặn các hành vi bất thường.

Trong một phiên RDP, có thể biết các trang web mà người dùng đã truy cập. Điều này đặc biệt hữu ích vì một số trang web có thể cung cấp phần mềm độc hại. Các trường hợp sử dụng bao gồm pháp y, kiểm soát phiên, v.v.

Thu thập các phiên truy cập Web

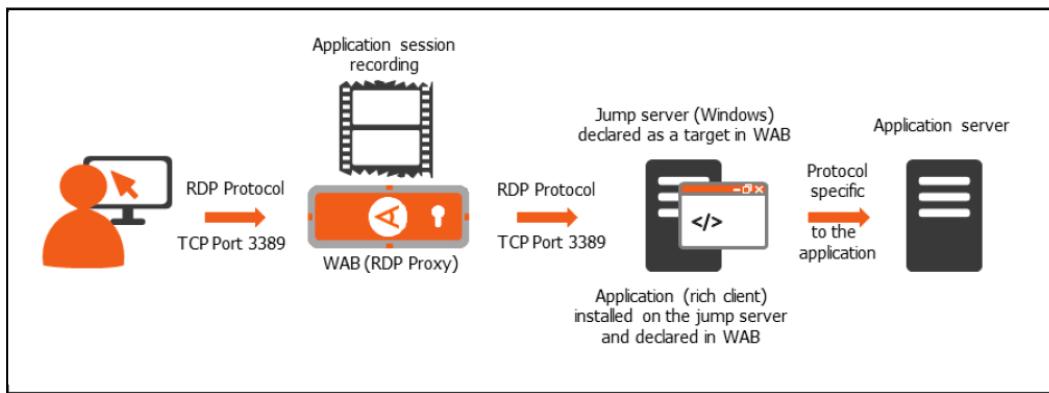
Khi người dùng truy cập Web trong phiên làm việc, Wallix Bastion có thể bắt được thông tin và lưu vào Metadata

```
[RDP Session] type = "WEB_DOCUMENT_COMPLETE" session_id = "SESSIONID-0000" client_ip = "192.168.1.10"
target_ip = "192.168.1.200" user = "Maint" device = "win2k8" service = "rdp" account = "supporter" url =
https://fr.wikipedia.org/
```

Như thế, hệ thống có thể giúp xác định xem người dùng có truy cập các trang web dính mã độc hay không.

5.7.2.6. Kiểm soát truy cập vào các ứng dụng chuyên biệt qua Jump Server

Kết nối với các ứng dụng được thực hiện khi máy chủ Jump Server nơi cài đặt ứng dụng quản trị của hệ thống cần quản trị. Máy chủ này là máy chủ Windows 2008 R2 trở lên có sẵn tính năng The “Terminal Services” và “Remote Desktop” cùng với CAL đủ cho số lượng kết nối.



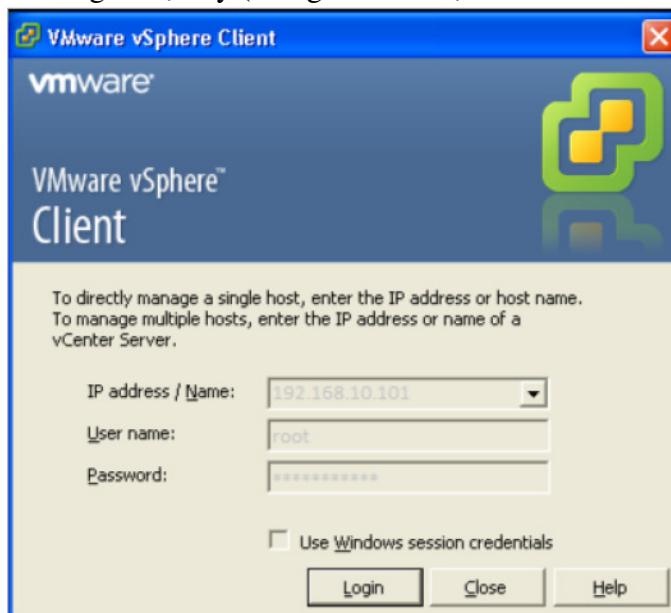
Để kết nối, người dùng kết nối tương tự như các kết nối bằng giao thức RDP. Điểm khác biệt chính là bạn phải chọn kết hợp mật khẩu / đăng nhập của ứng dụng đích (root @ VMware_ESX trong ví dụ này).

| Target Group | target |
|--------------|------------------------------|
| | |
| Win | administrateur@win2003:RDP |
| Win | administrateur@win2008R2:RDP |
| ESX | root@VMware_ESX:APP |

Lưu ý: giao thức được hiển thị cho tất cả các kết nối ứng dụng là APP thay vì RDP, cho phép bạn phân biệt chúng với các kết nối hệ thống (RDP).

| Protocol | Close Time |
|----------|------------|
| | |
| RDP | - |
| RDP | - |
| APP | - |

Sau đó, Bastion mở kết nối đến tài khoản VSphere đã chọn, nhập tổ hợp mật khẩu / đăng nhập thích hợp cho tài khoản - trong thư mục gốc trong ví dụ này (thông tin xác thực của tài khoản được lưu trữ trong Bastion).



Khi thông tin đăng nhập của tài khoản đích đã được gửi đến máy khách vSphere, bạn có thể sử dụng ứng dụng đích mà không cần biết mật khẩu của tài khoản gốc Root.

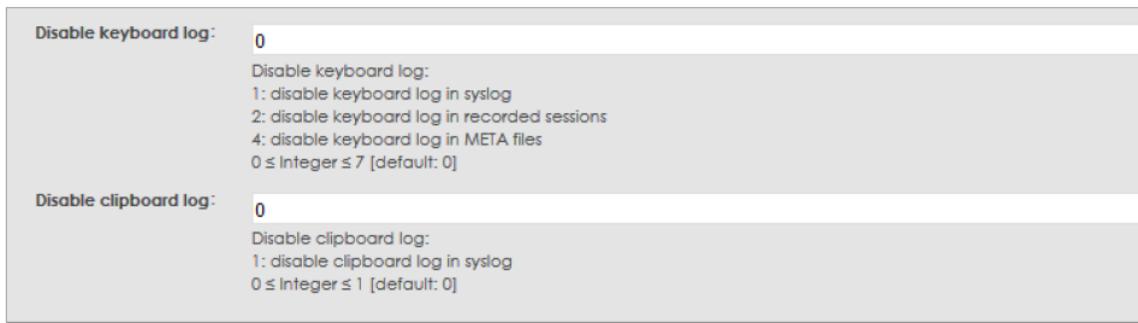
Bạn cũng có thể sử dụng màn hình lựa chọn Web và nhập vào ứng dụng cần thiết



Quá trình này tương tự như kết nối RDP tiêu chuẩn.

5.7.2.7. Kiểm soát bàn phím trong phiên truy cập

Wallix Bastion cho phép giám sát bàn phím trong phiên truy cập



Do đó, tất cả các dòng lệnh được nhập sẽ được ghi lại để phục vụ việc truy vết. Nhờ các dữ liệu này được ghi nhận theo thời gian thực, các hành vi bất thường có thể được phát hiện. Hệ thống có thể tự động ngắt phiên kết nối ngay khi người dùng có dấu hiệu gõ các lệnh không được phép.

5.7.2.8. Tự động ngắt kết nối nếu người dùng vi phạm chính sách bảo mật

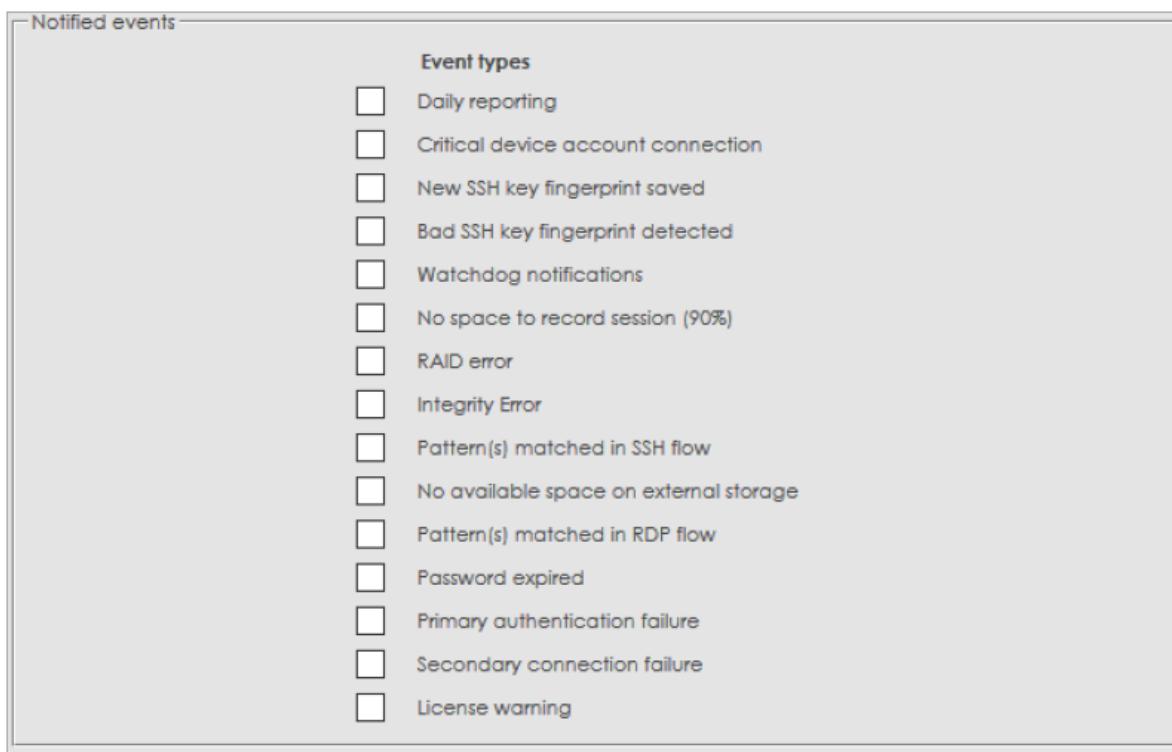
Hệ thống cho phép đưa ra cảnh báo nếu người dùng gõ những lệnh tiềm ẩn rủi ro cho hệ thống như lệnh “sudo” hoặc chạy các tiến trình (process) không được phép. Chức năng này cũng cho phép người quản trị sử dụng được với các giao thức RDP thông qua các dữ liệu thu thập được bởi Session Probe, tính năng OCR và log bàn phím.

WAB sẽ phân tích các kết quả này để xem xét liệu window “firewall” hay các file bí mật có bị truy cập không.

| Action | Rules | SubProtocol |
|--------|----------|---------------------------------|
| None | | SSH_SHELL_SESSION / X11_SESSION |
| kill | sudo | SSH_SHELL_SESSION / X11_SESSION |
| notify | Secret | RDP |
| kill | Firewall | RDP |

Người quản trị cũng có thể thiết lập các cảnh báo bảo mật như:

- Kết nối tới các tài khoản gốc quan trọng
- Thay đổi khóa SSH trên tài khoản thực của thiết bị
- Kết nối không thành công tới thiết bị quản trị.



5.7.2.9. Kiểm soát tệp được truyền vào và ra theo SSH/RDP

Đội ngũ kiểm tra đánh giá an toàn thông tin có thể xem trong một phiên, các tệp nào đã được chuyển và nếu chúng được lưu trữ bên trong Wallix Bastion khi tích hợp với DLP và AV thì chúng có thể được tải xuống để đánh giá.

5.7.3 Tính năng Session Sharing

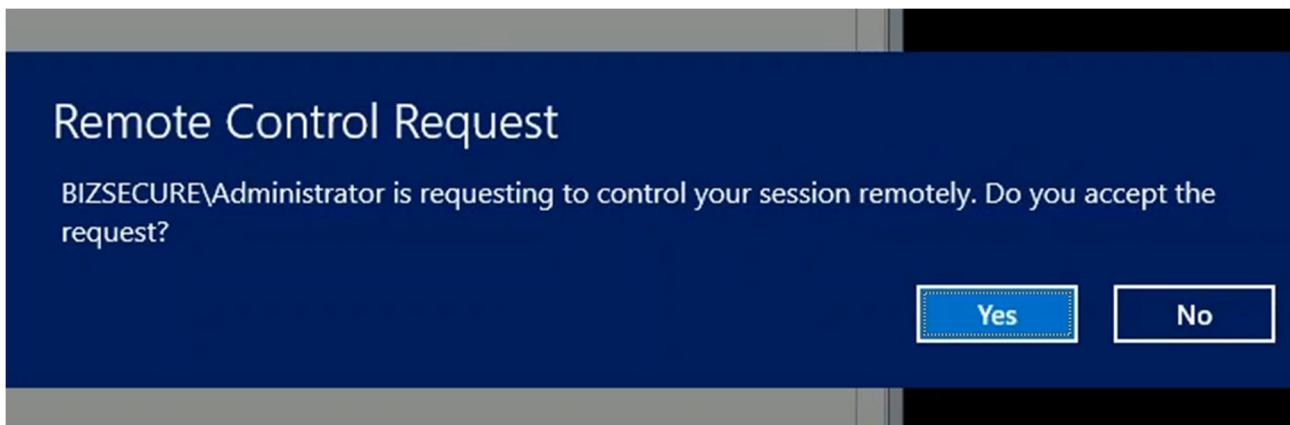
Wallix Bastion cho phép người dùng đang kết nối mời 1 người dùng khác cùng kết nối để hỗ trợ thêm. Người dùng được mời kết nối tạm gọi là Supporter hoàn toàn có thể thao tác trên hệ thống đang được kết nối. Hiện tính năng này hỗ trợ cho Windows Server 2008, 2012, 2016 và 2019.

The screenshot shows a list of sessions with the following details:

| | Status | User | Target | Target |
|--------------------------|-------------------|----------------------------------|--------------|-------------------|
| <input type="checkbox"/> | toan@192.168.56.1 | Administrator@local@Win2012:3389 | 192.168.56.1 | toan@192.168.56.1 |

Below the table, there is a button labeled "Control session with user's permission (Instant access)".

Ngay khi có người muốn tham gia vào chung phiên kết nối, người dùng sẽ nhận được thông báo:

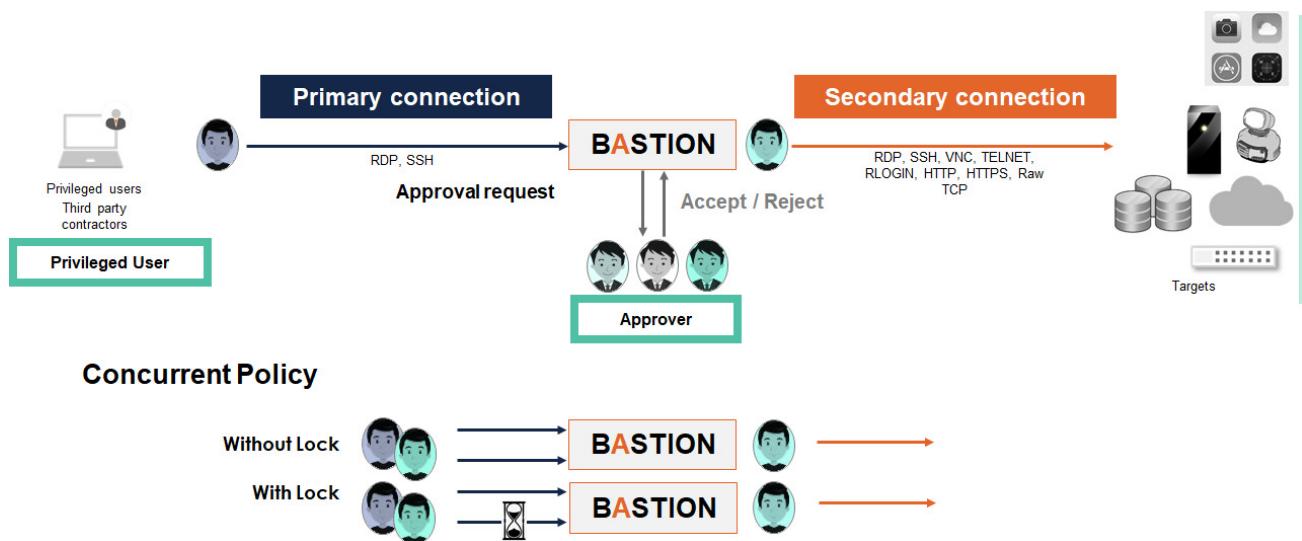


Nếu yêu cầu nhảy vào phiên được cho phép, cả 2 cùng có quyền điều khiển.

Hạn chế: Phiên bản hiện tại chưa phân biệt được đâu là hành vi của người dùng Supporter.

5.7.4 Hỗ trợ quy trình xác nhận (Workflow Approval)

Wallix Bastion hỗ trợ tính năng Workflow Approval. Tính năng này thường được áp dụng trên các hệ thống quan trọng, hạn chế tối đa việc kết nối không có lý do.



Tính năng này có thể bật tắt tùy theo nhóm thiết bị (Resource Group)

Approval workflow:

Comment: disabled optional mandatory

Ticket: disabled optional mandatory

Approvers:

| Available Approver group(s) | Chosen Approver group(s) |
|--|--|
| Elevated Permissions Help Desk SUser | Select your choice(s) and click Admin |

Quorum in authorized timeframes: 1
empty: approval workflow with automatic approval; 0: no approval workflow (direct connection); > 0: quorum to reach

Quorum out of authorized timeframes: 1
empty: approval workflow with automatic approval; 0: no connection allowed; > 0: quorum to reach

Ngay cả khi một tài khoản quản trị có quyền truy cập vào các hệ thống này, họ vẫn phải điền thông tin vào biểu mẫu xin phê duyệt ngay khi kết nối vào:

Information
Selected target: administrator@Windows2008-RDP
You need to ask for approval in order to connect to the target.
Duration * Format: [hours]:[mins]:[sec]
Ticket Ref. *
Comment *
(*) required fields
Confirm
Back to Selector **Exit**

Hoặc nếu có kế hoạch làm việc từ trước, việc xin phép có thể được gửi trước:

Sessions Passwords

| Protocol | Target | Authorization name | Account description | Target description | Time frame | Last connection | Approval |
|----------|----------------------------------|--------------------|---------------------|--------------------|---------------------|-----------------|----------|
| SSH | admin@local@Ubuntu2004:SSH | Admin-Linux | -- | allthetime | 2020-11-10 11:12:42 | | |
| RDP | administrator@local@W2k16-01:RDP | Windows-Servers | -- | allthetime | 2021-03-17 14:48:40 | | |
| RDP | administrator@local@W2k16-01:RDP | LDAP-Windows | -- | allthetime | 2021-03-17 14:48:40 | Request | |
| APP | robinhood@Firefox:APP | Windows-Servers | -- | allthetime | -- | | |
| APP | robinhood@Firefox:APP | LDAP-Windows | -- | allthetime | -- | Request | |
| APP | robinhood@MySQL_Workbench:APP | Windows-Servers | -- | allthetime | -- | | |
| APP | robinhood@MySQL_Workbench:APP | LDAP-Windows | -- | allthetime | -- | Request | |
| SSH | wabadmin@local@Linux:SSH | Admin-Linux | -- | allthetime | 2020-11-10 07:53:59 | | |

1 - 8 / 8

Approval request: robinhood → administrator@local@W2k16-01:RDP

Start date *: 2021-03-21
Start time *: 08:56
Duration *: 1h
Format: "[hours]:[mins]:[sec]" (each unit is optional)
Ticket reference *:
Comment *:
Request **Cancel**

Ngay khi yêu cầu gửi đi, người có trách nhiệm phê duyệt (Approver) sẽ nhận được email và tiến hành phê duyệt như được quy định trong Ủy quyền / Luồng công việc.

Wallix Bastion lưu giữ chi tiết thông tin các yêu cầu xin phép truy cập và lịch sử phê duyệt phục vụ cho việc kiểm toán.



| Status | Quorum | Ticket | User | Target | Beginning | End | Duration | Answers |
|----------|--------|--------|------|--------------------------------|---------------------|---------------------|----------|---------|
| accepted | 1 / 1 | 1234 | Rash | SuperAdmin@local@DC01:RDP | 2016-02-01 21:00:00 | 2016-02-01 22:00:00 | 1h | Jamie |
| accepted | 1 / 1 | 23456 | Rash | SuperAdmin@local@DC01:RDP | 2016-02-01 14:05:00 | 2016-02-01 14:15:00 | 10m | Jamie |
| accepted | 1 / 1 | 345678 | Rash | SuperAdmin@local@DC01:RDP | 2016-02-01 10:17:00 | 2016-02-01 10:27:00 | 10m | Jamie |
| accepted | 1 / 1 | 345678 | Rash | SuperAdmin@local@DC01:RDP | 2016-01-29 14:12:00 | 2016-01-29 14:32:00 | 20m | Jamie |
| accepted | 1 / 1 | 12345 | Rash | administrator@local@DC01:RDP | 2016-01-27 11:24:00 | 2016-01-27 11:34:00 | 10m | Jamie |
| accepted | 1 / 1 | 1234 | Rash | administrator@local@Win2k8:RDP | 2016-01-27 10:47:00 | 2016-01-27 10:57:00 | 10m | Jamie |

5.8. Vai trò của mô đun Password Manager

Như chúng tôi đề cập ở phần giải pháp, WAB lưu trữ các tài khoản gốc truy cập vào thiết bị.

Ngoài ra, nếu mô đun Password Manager được kích hoạt, Wallix Bastion cho phép:

- Check in/Check out mật khẩu. Mật khẩu sau khi được check out và check in trở lại sẽ được hệ thống tự thay đổi
- Tự động thay đổi mật khẩu định kỳ.

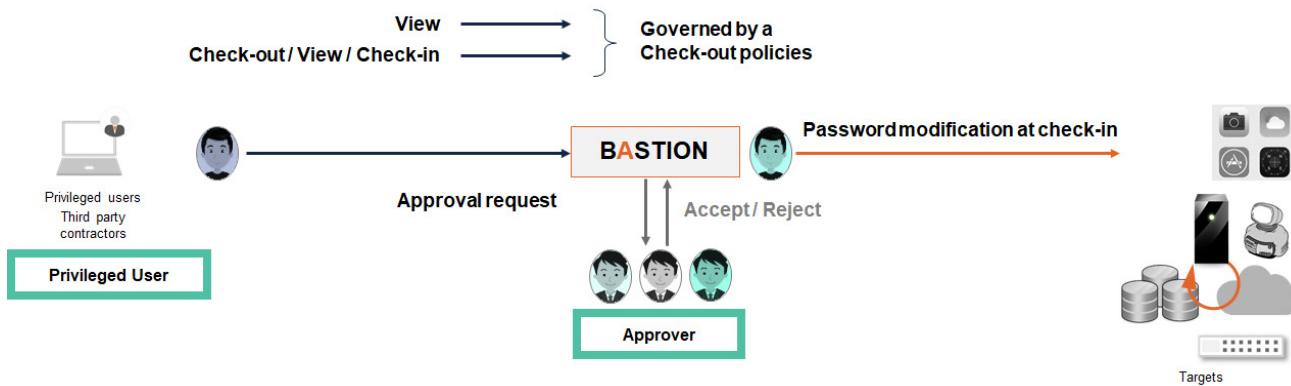
Mật khẩu mới được tạo ra sẽ tuân thủ chính sách về độ phức tạp của mật khẩu.

5.8.1 Quản lý xác thực tập trung với tính năng check in/ check out

Tính năng check out này cho phép sử dụng mật khẩu và tự động thay đổi khi check in.

Policy name * : checkout
 Description : Checkout Password
 Enable lock :
 The checkout duration does not apply for session management
 Checkout duration * : 30m
 Format: "[hours]h[mins]m" (each unit is optional)
 Checkout duration extension : 10m
 Format: "[hours]h[mins]m" (each unit is optional)
 Maximum checkout duration : 1h
 Format: "[hours]h[mins]m" (each unit is optional)
 Change password at check-in :

Tính năng Check out/Check in có thể kết hợp cùng quy trình xác nhận (Workflow Approval)



5.8.2 Tính năng tự động đổi mật khẩu

Tính năng này giúp mật khẩu truy cập vào thiết bị đầu cuối sau mỗi khoảng thời gian nhất định dựa theo chính sách bảo mật mật khẩu do người quản trị thiết lập (số lượng ký tự tối thiểu, sử dụng các ký tự đặc biệt....).

Wallix Bastion dùng cơ chế Plugin. Hiện Wallix Bastion đi kèm sẵn các plugin

- Windows OS
- Unix / Linux
- Cisco
- Oracle
- MySQL
- Fortinet Fortigate
- Juniper SRX
- Palo Alto PA-500
- IBM 3270
- Dell iDRAC
- LDAP

Các plugin có thể phát triển theo yêu cầu (tính phí và được thực hiện bởi các chuyên gia của Wallix)

Do đó, người quản trị có thể yên tâm rằng mật khẩu đổi với các tài khoản dịch vụ thực sự mạnh và được thay đổi theo định kỳ, giúp giảm nguy cơ tấn công “dictionary” (*tấn công từ điển là loại tấn công giải mã mật khẩu bằng việc cố gắng sử dụng các từ có nghĩa thay vì thử tất cả mọi khả năng*) và đáp ứng các yêu cầu về tiêu chuẩn thay đổi mật khẩu (ví dụ: mật khẩu cần thay đổi sau chu kỳ 30 ngày).

Chức năng thay đổi mật khẩu này có thể được cung cấp cho những người dùng ở những trường hợp đặc biệt như những nhà cung cấp dịch vụ bên ngoài khi cần thiết.

Để thực hiện tính năng này, ngoài license cho mô đun Password Manager, người quản trị Wallix Bastion sẽ cấu hình như sau:

The screenshot displays two pages from the WALLIX Bastion web interface:

- Edit account administrator (Top Window):**
 - General Tab:** Shows Device (W2k16-01), Local domain (local), Account name (administrator), and Account login (administrator).
 - Checkout policy:** Set to "default".
 - Resource association:** A table showing a service named "W2k16-01:RDP" associated with the device.
 - Buttons:** Close, Apply and continue, and Apply and close.
- Password management (Bottom Window):**
 - Password change policies Tab:** Shows a single policy named "Windows Password".
 - Edit password change policy Form:**
 - Policy name:** Windows Password.
 - Description:** (Empty text area).
 - Period of change:** Every month on every day of the month at every hour : every minute.
 - Policy type:** Set to "password".
 - Password generation Form:**
 - Password length:** 24.
 - Number of special characters:** 0 (empty = do not use these characters, 0 = no minimum).
 - Number of lower case letters:** 0 (empty = do not use these characters, 0 = no minimum).
 - Number of upper case letters:** 0 (empty = do not use these characters, 0 = no minimum).
 - Number of digits:** 0 (empty = do not use these characters, 0 = no minimum).
 - Forbidden characters:** (Empty text area).
 - Buttons:** Apply, Cancel.

WAB cho phép người dùng nhận email về những tài khoản quản trị gốc đã thay đổi, tuy nhiên WAB yêu cầu các tài khoản người dùng phải cung cấp các khóa GPG. Khóa GPG sẽ được dùng để mã hóa nội dung email chứa các mật khẩu gốc đã được thay đổi. Khi hệ thống gặp sự cố những người dùng này có thể sử dụng các khóa này để giải mã nội dung của email lấy lại mật khẩu gốc của thiết bị.



Create user

User name * : usrPasswordSafe

Display name :

Email * : passwordsafe@wallix

User's email

GPG key : Choose File No file chosen

Preferred language * : English ▾

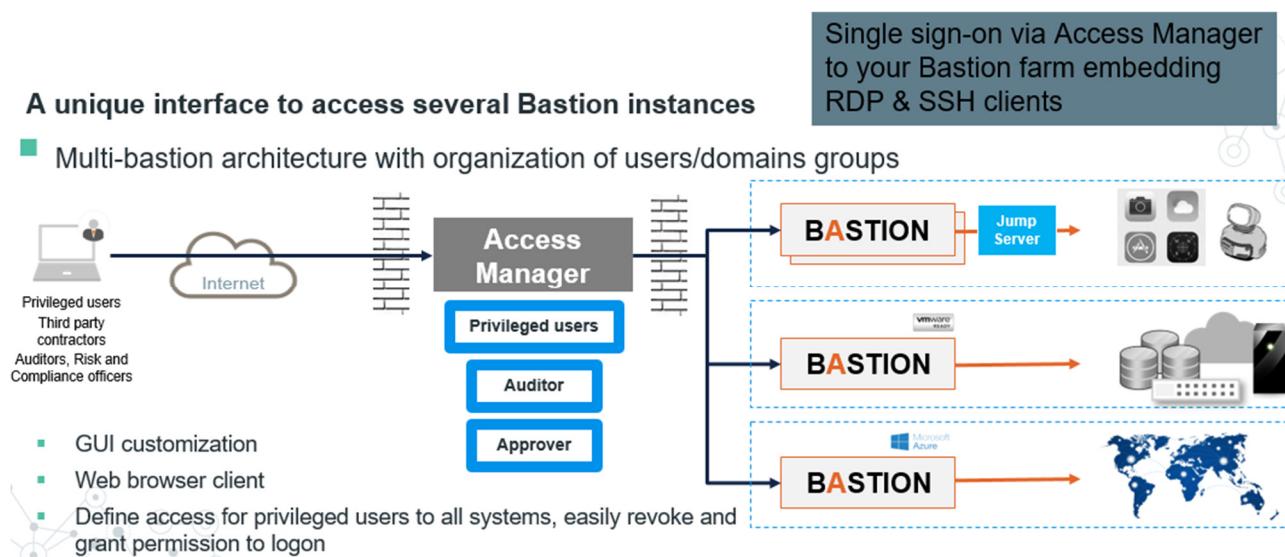
User's preferred lanauage

Profile * : prfCredRecovery ▾

Account expiration date :

YYYY-MM-DD hh:mm

5.9. Mô đun Access Manager (WAM)



Với mô đun WAM, hệ thống không cần cho phép các kết nối RDP, SSH hoặc Telnet từ ngoài. Chỉ cần thiết bị có trình duyệt HTML5 kết nối vào Access Manager với giao thức HTTPS, không cần cài đặt Plugin hay bất kỳ ứng dụng nào khác, không cần hạ tầng VPN, người dùng đặc quyền hoàn toàn có thể truy cập và quản trị hệ thống như ngồi trong mạng nội bộ.

5.9.2.1. Hỗ trợ multi-tenant

Một WAM hoàn toàn cho phép kết nối với nhiều Wallix Bastion bên trong. Mỗi Wallix Bastion có thể tùy biến giao diện cho phép nhận dạng. Nhờ đó, WAM có thể dùng trong các Data Center dùng chung.

5.9.2.2. Hỗ trợ xác thực qua SAML

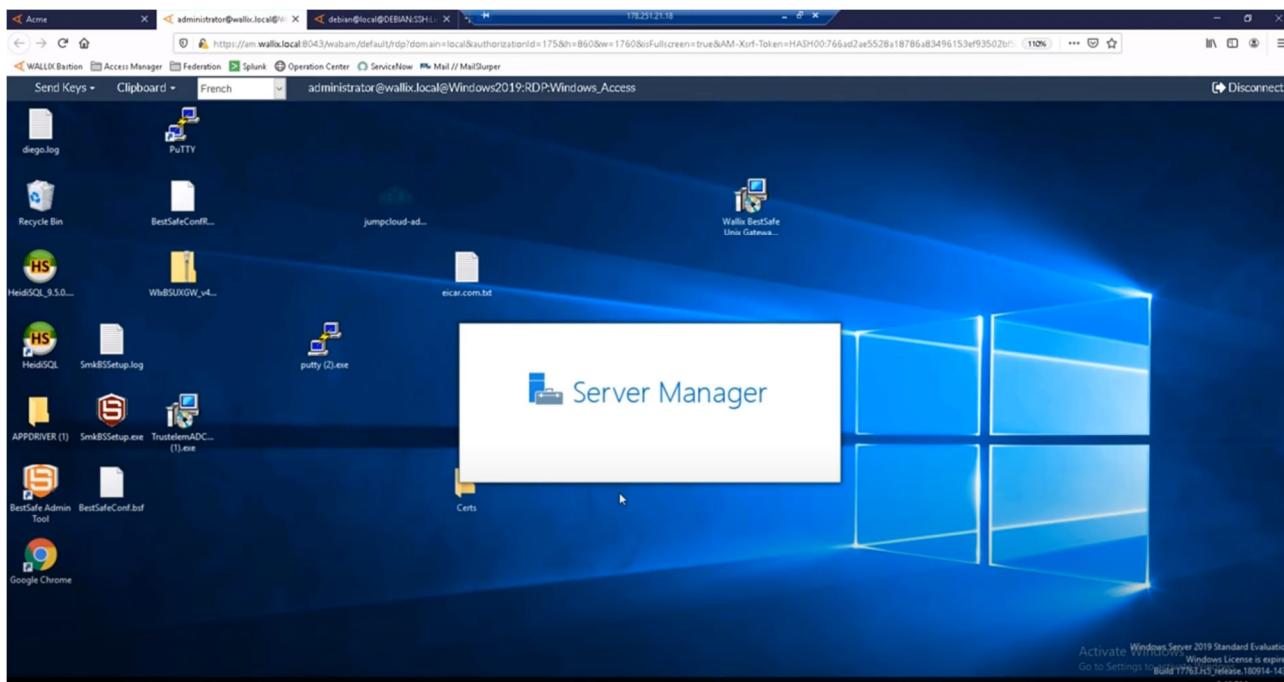
WALLIX Access Manager hỗ trợ tích hợp nhiều phương thức xác thực như cục bộ, Active Directory, LDAP, nhưng cũng có thể SAML như SafeNet, Okta, Trustelem, .v.v.

Mỗi tổ chức (tenant) bên trong WAM có thể có xác thực riêng với các miền khác nhau.

5.9.2.3. Kết nối SSH qua WAM

The screenshot displays two browser windows. The top window shows the 'Sessions' page with a sidebar for 'My Authorizations' containing items like Super_windows, Super_Root, Super_App, Super_Share, Super_Routers, super_linux, and Applications. A table lists a single session: Resource (Centos), Domain (local), Account (acme), Service (SSH), Name/Groups (Super_Linux), and Bastion (WAB5.0.2). The bottom window shows a terminal session titled 'acme@localhost:~\$'. It displays a welcome message from Wallix AdminBastion, a security notice about recorded actions, and a timestamp of 'Last login: Wed Jan 11 18:35:28 2017 from 192.168.10.5'. The user is currently at the prompt '|acme@localhost ~|\$'.

5.9.2.4. Kết nối RDP qua WAM



5.10. Tích hợp hoàn hảo với các hệ thống SIEM, IDS, và SOAR

SIEM: Security information and event management – Hệ thống giám sát an ninh mạng: là hệ thống được thiết kế nhằm thu thập và phân tích nhật ký, các sự kiện an ninh từ các thiết bị đầu cuối và được lưu trữ tập trung.

IDS: intrusion detection system (Hệ thống phát hiện xâm nhập): là hệ thống giám sát mạng hoặc hệ thống máy tính về những hoạt động ác ý hoặc các vi phạm chính sách

SOAR: Security Orchestration, Automation and Response - giải pháp thu thập dữ liệu về các mối đe dọa bảo mật và chống lại các cuộc tấn công bảo mật nhỏ mà không cần sự sự giúp đỡ, điều khiển của con người.

Việc sử dụng PAM với hệ thống SIEM và SOAR tạo ra một hệ thống cho phép gửi cảnh báo nhanh và mạnh mẽ. Các hệ thống như trên sẽ đóng vai trò phân tích tự động. Nếu có cuộc tấn công xảy ra, hệ thống này sẽ gửi chúng cho chuyên viên phân tích bảo mật. Chuyên viên này sẽ sử dụng giải pháp PAM để kiểm tra phiên đặc quyền liên quan tới cuộc tấn công này. Họ sẽ ngay lập tức biết được các bí nhí phân đáng ngờ đã được cài đặt trên hệ thống tại thời điểm cụ thể và bởi người dùng nào. Điều này cho phép chúng ta biết được tài khoản đặc quyền nào đã bị tấn công.

Giải pháp Wallix Bastion sẽ chuyển các dữ liệu sau cho SIEM/SOAR mà không cần bất kỳ phần mềm bên thứ 3 nào được cài đặt để chuyển nhật ký.

- Thay đổi cấu hình (log)
- Xác thực (log)
- Hoạt động của kho mật khẩu – password vault (log)
- Sự kiện proxy SSH (log)
- Sự kiện proxy RDP (log)
- Phiên SSH (metadata)
- Phiên RDP (metadata)
- Phiên VNC (metadata)

Kết hợp với các video về phiên truy cập cho phép người quản trị, nhà phân tích bảo mật biết được từng bước cấu hình của người dùng sau khi được cấp đặc quyền truy cập, giúp họ hỗ trợ việc điều tra nhanh chóng và chính xác các cuộc tấn công, điều này đặc biệt có ích đối với trường hợp hệ thống bị tấn công mất cấu hình, hay bị chèn dữ liệu giả mạo.

5.11. Báo cáo

Bastion-SM bao gồm một mô-đun báo cáo tích hợp để xử lý thông tin được cung cấp trong nhật ký kết nối. Các báo cáo có thể tùy biến bằng các bộ lọc:

Báo cáo cũng có thể được tạo ở định dạng CSV (ví dụ: nhật ký kết nối, nhật ký xác thực, v.v.) để đưa vào các công cụ khác như bảng điều khiển, v.v.

| | A | B | C | D | E |
|----|--------------------------------|---------|---------|--------|---|
| 1 | | Overall | Success | Failed | |
| 2 | Grant@CMD | 3 | 3 | 0 | |
| 3 | admin@Linux1:SSH_X11_SESSION | 13 | 13 | 0 | |
| 4 | admin@Linux2:SSH_X11_SESSION | 1 | 1 | 0 | |
| 5 | Grant@Secure_Internet | 1 | 1 | 0 | |
| 6 | administrator@Windows1:RDP | 3 | 3 | 0 | |
| 7 | administrator@Windows2008:RDP | 3 | 3 | 0 | |
| 8 | administrator@Windows2:RDP | 1 | 1 | 0 | |
| 9 | administrator@Windows_2012:RDP | 10 | 10 | 0 | |
| 10 | administrator@Windows_2:RDP | 5 | 5 | 0 | |
| 11 | | | | | |
| 12 | | | | | |

5.12. Hỗ trợ REST API

Wallix Bastion cung cấp REST API đầy đủ cho phép tích hợp với các hệ thống khác.

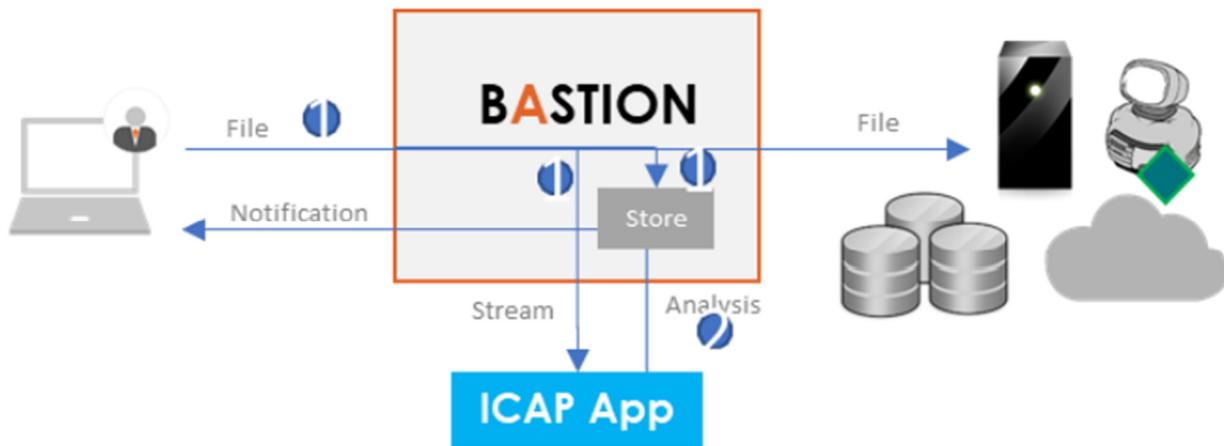
- Xác thực Kerberos trên API
- Quản lý thông tin xác thực nhất quán (Thông tin xác thực tài khoản thiết bị, miền và ứng dụng)
- Ghi một dòng vào tệp kiểm toán (Log SIEM)
- Quản lý trên một nhóm người dùng và mục tiêu, mô hình tiêu diệt / thông báo
- Chính sách mật khẩu cục bộ
- Truyền mật khẩu và khóa SSH đến các mục tiêu (Tài khoản Thay đổi mật khẩu)
- Cấu hình và tùy chọn (chỉ đọc)
- Liệt kê người dùng LDAP
- Quản lý khóa API
- Cấu hình CRL / OCSP / X509
- Cấu hình SMTP
- Yêu cầu phiên X509
- Thay đổi mật khẩu người dùng
- Hỗ trợ MFA (RADIUS, PingID)

5.13. Tích hợp giải pháp Anti-virus, DLP

Wallix Bastion cho phép tích hợp với các giải pháp Anti-Virus và chống thất thoát dữ liệu (DLP) bằng cách kết nối với các giải pháp này qua giao thức ICAP. Kết nối có thể được bảo mật thông qua tùy chọn TLS.

Hiện Wallix Bastion hỗ trợ 2 kết nối ICAP:

- Truyền tệp lên các hệ thống được quản trị. Wallix Bastion sẽ kết nối với giải pháp Anti-Virus để kiểm tra.
- Khi tệp được tải ngược ra, hệ thống DLP kết nối với Wallix Bastion sẽ kiểm tra.



Wallix Bastion cho phép cấu hình:

- Hoặc tất cả tệp đều được lưu lại cho mục đích Audit
- Hoặc chỉ lưu lại các tệp có kết quả đáng ngờ do DLP và AV phản hồi lại,

Wallix Bastion có thể tích hợp bất kỳ phần DLP và AV nào hỗ trợ ICAP. Tính năng này đã được kiểm thử với các giải pháp Antivirus / DLP sau: Kaspersky, McAfee, Forcepoint, Falcongaze và ClamAV.

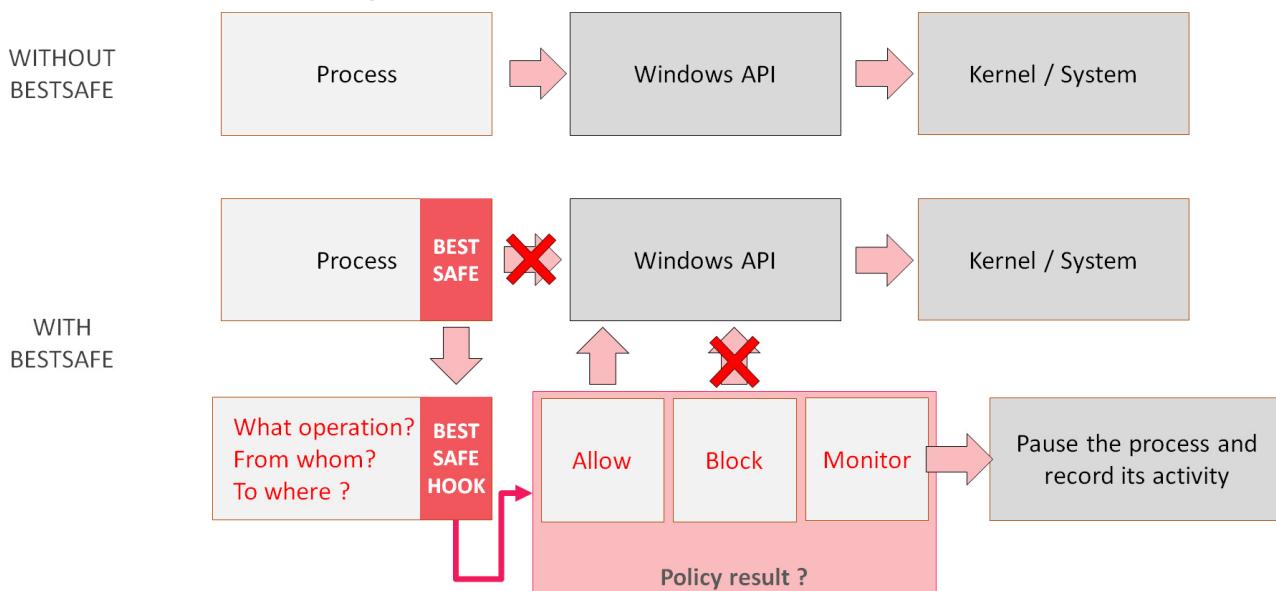
Hạn chế:

- Không hỗ trợ tính năng này cho việc truyền tệp với giao thức VNC.
- Chặn tệp đã chuyển khi tính năng DLP / AV trả về kết quả đáng ngờ không phải là một phần của các phiên bản Wallix Bastion hiện nay. Tính năng này tiếp tục được phát triển trong các phiên bản nâng cấp tiếp theo.

5.14. Mô đun BestSafe

BestSafe là giải pháp PEDM của Wallix nó có thể chạy độc lập; nhưng đồng thời tích hợp với Wallix Session Manager trong Wallix Bastion để thực thi các chính sách kiểm soátEndPoint và chuyển log về cho Wallix Bastion

5.14.3 Cách thức hoạt động của BestSafe



BestSafe được triển khai dưới dạng Agent trên cácEndPoint. Khi có BestSafe, mọi process mở ra đều bị BestSafe kiểm tra và chặn nếu chính sách đã được thiết lập sẵn không cho phép chạy process này. Nếu process được phép chạy, BestSafe sẽ giám sát process này và ghi nhận các hoạt động liên quan đến process này.

BestSafe cho phép không cần cung cấp các tài khoản đặc quyền cho người dùng trên máy trạm. Quản trị hệ thống chỉ cần cấu hình sẵn ủy quyền. Khi người dùng chạy các tiến trình cần có đặc quyền đã được cho phép, BestSafe sẽ tự động thực hiện việc này mà không cần người dùng đang truy cập phải thao tác gì thêm (Transparent).

Các tiến trình được phép chạy vẫn bị BestSafe giám sát và kiểm soát các API được gọi. Các API này có thể chặn nếu được cấu hình trong BestSafe.

5.14.4 Tính năng của BestSafe

- Quản lý đặc quyền ở cấp tiến trình (Process)
- Quản lý danh sách đen các ứng dụng (Blacklist)
- Nâng cao đặc quyền ứng dụng nếu cần và dựa trên chính sách được thiết lập.
- Buộc các ứng dụng chạy mà không cần có đặc quyền
- Chặn các hàm API mã hóa dữ liệu được gọi (chống Crypto API liên quan đến các Malware mã hóa dữ liệu)
- Giám sát việc truy cập các thư mục nội bộ và trong mạng.
- Giám sát và kiểm soát các process
- Quản lý Group, User cục bộ trên máy trạm bao gồm thay đổi mật khẩu
- Hỗ trợ tích hợp với Active Directory
- Phân tích & báo cáo, cảnh báo, tích hợp SIEM