**TCVN** **T I Ê U C H U Ẩ N Q U Ố C G I A**

**TCVN xxxx:2023**

**Xuất bản lần 1**

**CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - HỒ SƠ BẢO VỆ CHO SẢN PHẨM TƯỜNG LỬA ỨNG DỤNG WEB**

***Information technology - Security techniques –***

***Protection profile for Web Application Firewall***

**HÀ NỘI - 2023**

**Mục lục**

[1 Phạm vi áp dụng 8](#_Toc137475265)

[2 Tài liệu viện dẫn 8](#_Toc137475266)

[3 Thuật ngữ và định nghĩa 8](#_Toc137475267)

[4 Ký hiệu và thuật ngữ viết tắt 13](#_Toc137475268)

[5 Giới thiệu Hồ sơ bảo vệ 14](#_Toc137475269)

[5.1 Tổng quan về TOE 15](#_Toc137475270)

[5.1.1 Tổng quan về tường lửa ứng dụng web 15](#_Toc137475271)

[5.1.2 Phạm vi và loại TOE 15](#_Toc137475272)

[5.1.3 Sử dụng TOE và các tính năng bảo mật chính 15](#_Toc137475273)

[5.1.4 Môi trường hoạt động không phải TOE và TOE 15](#_Toc137475274)

[5.2 Quy ước 19](#_Toc137475275)

[6 Các yêu cầu tuân thủ 19](#_Toc137475276)

[6.1 Yêu cầu tuân thủ CC 19](#_Toc137475277)

[6.2 Yêu cầu tuân thủ PP 20](#_Toc137475278)

[6.3 Yêu cầu tuân thủ gói 20](#_Toc137475279)

[6.4 Cơ sở yêu cầu tuân thủ 20](#_Toc137475280)

[6.5 Tuyên bố tuân thủ PP 20](#_Toc137475281)

[7 Các mục tiêu an toàn 20](#_Toc137475282)

[7.1 Các mục tiêu an toàn cho môi trường hoạt động 20](#_Toc137475283)

[8 Các yêu cầu chức năng an toàn 21](#_Toc137475284)

[8.1 Yêu cầu chức năng an toàn (SFR bắt buộc) 24](#_Toc137475285)

[8.1.1 Kiểm toán an toàn (FAU) 25](#_Toc137475286)

[8.1.2 Hỗ trợ mật mã (FCS) 31](#_Toc137475287)

[8.1.3 Bảo vệ dữ liệu người dùng (FDP) 34](#_Toc137475288)

[8.1.4 Định danh và xác thực (FIA) 38](#_Toc137475289)

[8.1.5 Quản lý bảo mật (FMT) 43](#_Toc137475290)

[8.1.6 Bảo vệ TSF (FPT) 55](#_Toc137475291)

[8.1.7 Truy cập TOE (FTA) 63](#_Toc137475292)

[8.2 Các yêu cầu chức năng an toàn (SFR bắt buộc có điều kiện) 64](#_Toc137475293)

[8.2.1 Kiểm toán bảo mật (FAU) 66](#_Toc137475294)

[8.2.2 Định danh và xác thực (FIA) 68](#_Toc137475295)

[8.2.3 Bảo vệ TSF (FPT) 69](#_Toc137475296)

[8.2.4 Truy cập TOE (FTA) 71](#_Toc137475297)

[8.2.5 Đường dẫn/kênh tin cậy (FTP) 73](#_Toc137475298)

[8.3 Yêu cầu chức năng an toàn (SFR tùy chọn) 75](#_Toc137475299)

[8.3.1 Hỗ trợ mật mã (FCS) 75](#_Toc137475300)

[8.3.2 Bảo vệ TSF (FPT) 76](#_Toc137475301)

[9 Yêu cầu đảm bảo an toàn 76](#_Toc137475302)

[9.1 Bảo mật Đánh giá mục tiêu 77](#_Toc137475303)

[9.1.1 Giới thiệu ASE\_INT.1 ST 77](#_Toc137475304)

[9.1.2. ASE\_CCL.1 Yêu cầu tuân thủ 78](#_Toc137475305)

[9.1.3. ASE\_OBJ.1 Mục tiêu bảo mật cho môi trường hoạt động 80](#_Toc137475306)

[9.1.4. ASE\_ECD.1 Định nghĩa thành phần mở rộng 80](#_Toc137475307)

[9.1.5. ASE\_REQ.1 Các yêu cầu bảo mật đã nêu 82](#_Toc137475308)

[9.1.6. Đặc tả tóm tắt ASE\_TSS.1 TOE 83](#_Toc137475309)

[9.2. Phát triển 83](#_Toc137475310)

[9.2.1. ADV\_FSP.1 Đặc tả chức năng cơ bản 83](#_Toc137475311)

[9.3. Tài liệu hướng dẫn 84](#_Toc137475312)

[9.3.1. AGD\_OPE.1 Hướng dẫn sử dụng vận hành 84](#_Toc137475313)

[9.3.2. AGD\_PRE.1 Quy trình chuẩn bị 86](#_Toc137475314)

[9.4. Hỗ trợ vòng đời 87](#_Toc137475315)

[9.4.1. ALC\_CMC.1 Dán nhãn cho TOE 87](#_Toc137475316)

[9.4.2. Phạm vi ALC\_CMS.1 TOE CM 87](#_Toc137475317)

[9.5. Thử nghiệm 88](#_Toc137475318)

[9.5.1. ATE\_FUN.1 Kiểm tra chức năng 88](#_Toc137475319)

[9.5.2. ATE\_IND.1 Thử nghiệm độc lập - tuân thủ 89](#_Toc137475320)

[9.6. Đánh giá lỗ hổng 89](#_Toc137475321)

[9.6.1. Khảo sát lỗ hổng AVA\_VAN.1 90](#_Toc137475322)

[Phụ lục 91](#_Toc137475323)

[(Quy định) Các định nghĩa thành phần mở rộng 91](#_Toc137475324)

[1. Hỗ trợ mật mã 91](#_Toc137475325)

[2. Bảo vệ dữ liệu người dùng 91](#_Toc137475326)

[3. Quản lý an toàn 93](#_Toc137475327)

[4. Bảo vệ TSF 94](#_Toc137475328)

[5. Cập nhật TSF 96](#_Toc137475329)

[Tài liệu tham khảo 98](#_Toc137475330)

1. **Lời nói đầu**
2. TCVN xxxx:2023 được xây dựng dựa trên cơ sở tham khảo “Korean National Protection Profile Web Application Firewall” của Viên nghiên cứu an ninh quốc gia Hàn Quốc, phiên bản 3.0, ngày 27/4/2023.
3. TCVN xxxx:2023 do Cục An toàn thông tin biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

**Công nghệ thông tin - Các kỹ thuật an toàn - Hồ sơ bảo vệ cho sản phẩm tường lửa ứng dụng web**

TIÊU CHUẨN QUỐC GIA TCVN xxxx:2023

*Information Technology - Security techniques - Protection Profile Web Application Firewall*

* 1. Phạm vi áp dụng

Tiêu chuẩn này quy định hồ sơ bảo vệ cho sản phẩm tường lửa ứng dụng web, thể hiện các yêu cầu chức năng an toàn (SFR) và yêu cầu đảm bảo an toàn (SAR) đối với sản phẩm tường lửa ứng dụng web.

Tiêu chuẩn này áp dụng vào quá trình đánh giá an toàn thông tin đối với sản phẩm tường lửa ứng dụng web theo các tiêu chí đánh giá được quy định trong TCVN 8709-1:2011 (ISO/IEC 15408-1:2009), TCVN 8709-2:2011 (ISO/IEC 15408-2:2008) và TCVN 8709-3:2011 (ISO/IEC 15408-3:2008).

* 1. Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây là cần thiết để áp dụng đối với tiêu chuẩn này. Đối với tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất (bao gồm cả phiên bản sửa đổi, bổ sung).

TCVN 8709-1:2011 (ISO/IEC 15408-1:2009), “Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 1: Giới thiệu và mô hình tổng quát”.

TCVN 8709-2:2011 (ISO/IEC 15408-2:2008), “Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 2: Các thành phần chức năng an toàn”.

TCVN 8709-3:2011 (ISO/IEC 15408-3:2008), “Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 3: Các thành phần đảm bảo an toàn”.

TCVN 11386:2016 (ISO/IEC 18045:2008), “Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp đánh giá an toàn công nghệ thông tin” [CEM].

* 1. Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong TCVN 8709-1:2011 và các thuật ngữ sau:

**Tài sản**

Các đối tượng mà chủ sở hữu của TOE gán giá trị lên

**Lựa chọn**

Đặc điểm kỹ thuật của một tham số được xác định trong một thành phần (của CC) hoặc yêu cầu

**Tiềm năng tấn công**

Đo lường nỗ lực được sử dụng để tấn công TOE được thể hiện dưới dạng chuyên môn, tài nguyên và động cơ của kẻ tấn công

**Tăng cường**

Bổ sung một hoặc nhiều yêu cầu cho một gói

**Dữ liệu xác thực**

Thông tin được sử dụng để xác minh danh tính được xác nhận của người dùng

**Phục hồi tự động**

Khôi phục mà không cần sự can thiệp của người dùng

**Quản trị viên được ủy quyền**

Người dùng được ủy quyền để vận hành và quản lý TOE một cách an toàn

**Có thể (Can/could)**

Có thể được trình bày trong Lưu ý áp dụngbiểu thị các yêu cầu tùy chọn được áp dụng cho TOE theo lựa chọn của Người yêu cầu đánh giá

**Lớp**

Tập hợp các họ CC chia sẻ một tiêu điểm chung

**Thành phần**

Tập hợp nhỏ nhất có thể lựa chọn các phần tử mà các yêu cầu có thể dựa trên đó

**DBMS (Hệ thống quản lý cơ sở dữ liệu)**

Một hệ thống phần mềm được cấu tạo để cấu hình và áp dụng cơ sở dữ liệu.

**Giải mã**

Hành động khôi phục bản mã thành bản rõ bằng cách sử dụng khóa giải mã

**Sự phụ thuộc**

Mối quan hệ giữa các thành phần sao cho nếu một yêu cầu dựa trên thành phần phụ thuộc được bao gồm trong một PP, ST hoặc gói, thì một yêu cầu dựa trên thành phần phụ thuộc đó thông thường cũng phải được bao gồm trong tuyên bố PP, ST hoặc gói

**Phần tử**

không thể chia cắt của một nhu cầu bảo mật

**Mã hóa**

Hành động chuyển đổi bản rõ thành bản mã bằng cách sử dụng khóa mã hóa

**Mức độ đảm bảo đánh giá (EAL)**

Tập hợp các yêu cầu đảm bảo rút ra từ CC Phần 3, đại diện cho một điểm trên thang đo đảm bảo xác định trước CC, tạo thành một gói đảm bảo

**Thực thể bên ngoài**

Con người hoặc thực thể CNTT có thể tương tác với TOE từ bên ngoài TOE ranh giới

**Họ**

Tập hợp các thành phần chia sẻ mục tiêu tương tự nhưng khác nhau về mức độ nhấn mạnh hoặc tính nghiêm ngặt

**Danh tính**

Biểu diễn xác định duy nhất các thực thể (ví dụ: người dùng, quy trình hoặc đĩa) trong ngữ cảnh của TOE

**Lặp lại**

Sử dụng cùng một thành phần để thể hiện hai hoặc nhiều yêu cầu riêng biệt

**Truy cập cục bộ**

Truy cập vào TOE bằng cách sử dụng cổng bảng điều khiển để quản lý TOE bởi quản trị viên, trực tiếp

**Quyền truy cập quản lý**

Quyền truy cập vào TOE bằng cách sử dụng HTTPS, SSH, TLS, v.v. để quản lý TOE bởi quản trị viên, từ xa

**Bảng điều khiển quản lý**

Chương trình ứng dụng cung cấp GUI, CLI, v.v. cho quản trị viên và cung cấp cấu hình và quản lý hệ thống

**Khôi phục thủ công**

Khôi phục thông qua máy chủ cập nhật, v.v. do người dùng thực hiện hoặc can thiệp của người dùng

**Đối tượng**

Thực thể thụ động trong TOE chứa hoặc nhận thông tin và trên đó các chủ thể thực hiện các thao tác

**Hoạt động (trên một thành phần của CC)**

Sửa đổi hoặc lặp lại một thành phần. Các hoạt động được phép trên các thành phần là gán, lặp, sàng lọc và lựa chọn

**Thao tác (trên một đối tượng)**

Loại hành động cụ thể được thực hiện bởi một chủ thể trên một đối tượng

**Chính sách bảo mật của tổ chức**

Tập hợp các quy tắc, thủ tục hoặc hướng dẫn bảo mật cho một tổ chức trong đó tập hợp này hiện được cung cấp bởi các tổ chức thực tế hoặc ảo hoặc sẽ được cung cấp

**Khóa riêng**

Một khóa mật mã được sử dụng trong thuật toán mật mã bất đối xứng và được TOEciated duy nhất với một thực thể (chủ thể sử dụng khóa riêng), không được tiết lộ

**Hồ sơ bảo vệ (PP)**

tuyên bố độc lập về nhu cầu bảo mật cho một loại TOE

**Thuật toán mã hóa khóa công khai (bất đối xứng)**

Thuật toán mã hóa sử dụng một cặp khóa công khai và khóa riêng

**RADIUS (Dịch vụ người dùng quay số xác thực từ xa)**

Thực hiện định danh và xác thực người dùng bằng cách gửi thông tin như ID người dùng, mật khẩu, địa chỉ IP đến máy chủ xác thực, khi người dùng từ xa yêu cầu quyền truy cập

**Trình tạo bit ngẫu nhiên (RBG)**

Một thiết bị hoặc thuật toán tạo ra một chuỗi nhị phân độc lập về mặt thống kê và không bị sai lệch. RBG được sử dụng cho ứng dụng mật mã thường tạo ra chuỗi bit 0 và 1 và chuỗi này có thể được kết hợp thành một khối bit ngẫu nhiên. RBG được phân loại thành loại xác định và không xác định. RBG loại xác định bao gồm một thuật toán tạo chuỗi bit từ giá trị ban đầu được gọi là “khóa gốc” và RBG loại không xác định tạo ra đầu ra phụ thuộc vào nguồn vật lý không thể đoán trước.

**Khuyến nghị/được khuyến nghị**

'Khuyến nghị' hoặc 'được khuyến nghị' được trình bày trong Lưu ý áp dụngkhông bắt buộc được khuyến nghị, nhưng bắt buộc phải được áp dụng cho các hoạt động an toàn của TOE

**Tinh chỉnh**

Bổ sung chi tiết cho một thành phần

**Vai trò**

Bộ quy tắc được xác định trước về các tương tác được phép giữa một người dùng và TOE

**Khóa bí mật**

Khóa mật mã được sử dụng trong thuật toán mật mã đối xứng và được TOEciated duy nhất với một hoặc một số thực thể, không được tiết lộ

**Bộ quy tắc Chính sách chức năng bảo mật (SFP)**

mô tả hành vi bảo mật cụ thể do TSF thực thi và có thể biểu thị dưới dạng một bộ SFR

**Đích an toàn (ST)**

Tuyên bố phụ thuộc vào việc triển khai các nhu cầu an toàn cho một TOE được xác định cụ thể

**Lựa chọn**

Đặc tả của một hoặc nhiều mục từ danh sách trong một thành phần

**Tự kiểm tra**

Kiểm tra trước khi vận hành hoặc kiểm tra có điều kiện được thực hiện bởi mô-đun mật mã

**Phải (Shall/must)**

'Shall' hoặc 'must' được trình bày trong Lưu ý áp dụngcho biết các yêu cầu bắt buộc được áp dụng cho TOE

**SSL (Lớp cổng bảo mật)**

Do Netscape phát triển, được đề xuất để cung cấp bảo mật như bảo mật và toàn vẹn trên mạng máy tính và được tiêu chuẩn hóa thành Bảo mật tầng vận chuyển (TLS).

**Đối tượng**

Bổ sung một hoặc nhiều yêu cầu vào một gói

**Kỹ thuật mật mã đối xứng**

Sơ đồ mã hóa sử dụng cùng một khóa bí mật trong chế độ mã hóa và giải mã, còn được gọi là kỹ thuật mã hóa khóa bí mật

**Mục tiêu đánh giá (TOE)**

Bộ phần mềm, phần sụn và /hoặc phần cứng có thể đi kèm với hướng dẫn

**Thực thể Tác nhân**

Đe dọa có thể hành động bất lợi đối với tài sản

**TLS (Bảo mật Tầng Giao vận)**

Đây là giao thức liên lạc an toàn giữa máy chủ và máy khách dựa trên SSL và được mô tả trong RFC 2246.

**Chức năng Bảo mật TOE (TSF)**

Chức năng kết hợp của tất cả phần cứng, phần mềm và phần sụn của TOE phải được dựa vào để thực thi chính xác các SFR

**Dữ liệu TSF**

Dữ liệu cho hoạt động của TOE mà việc thực thi SFR dựa vào đó

**Người dùng**

Xem “thực thể bên ngoài”, người dùng trong máy chủ xác thực mạng LAN không dây sẽ là quản trị viên được ủy quyền, trong khi người dùng trong ứng dụng khách xác thực mạng LAN không dây sẽ là người dùng cuối được ủy quyền

**Dữ liệu người dùng**

Dữ liệu cho người dùng, dữ liệu này không ảnh hưởng đến hoạt động của TSF

**Ứng dụng web**

Các ứng dụng được truy cập thông qua mạng như internet hoặc mạng nội bộ. Các ứng dụng thường được vận hành trong trình duyệt web hoặc môi trường có thể được kiểm soát bởi trình duyệt web và được hình thành bằng cách tích hợp các ngôn ngữ đánh dấu như HTML bằng cách sử dụng các ngôn ngữ lập trình có thể chạy trên trình duyệt web bao gồm JavaScript, Java Applet, v.v..

**Nội dung web**

Các tài liệu kỹ thuật số và nội dung đa phương tiện được phân phối qua web. Tài liệu kỹ thuật số bao gồm các tệp tài liệu web, tệp hình ảnh, v.v. và nội dung đa phương tiện bao gồm các tệp hoạt hình và video, v.v..

**Máy chủ web**

Phần mềm máy chủ web nhận thông tin được yêu cầu của máy khách (trình duyệt web) thông qua giao thức HTTP và chuyển kết quả trở lại khách hàng. Nó nhận tài nguyên được yêu cầu của khách hàng dưới dạng URL (Bộ định vị tài nguyên thống nhất) và xử lý nó bằng cách ánh xạ nó với hệ thống tệp nội bộ hoặc khi nhận URL và giá trị đầu vào (ví dụ: ID, mật khẩu, v.v. tại màn hình đăng nhập) cùng nhau, xử lý nó như đã thỏa thuận trước đó và gửi kết quả cho khách hàng. Apache, nginx và Microsoft IIS (Dịch vụ thông tin Internet) là một số máy chủ web tiêu biểu nhất.

Người dùng có quyền quản lý để cấu hình hoặc cập nhật TOE.

* 1. Ký hiệu và thuật ngữ viết tắt

|  |  |  |
| --- | --- | --- |
| AEAD | Chuẩn mật mã hóa có xác thực với dữ liệu được liên kết | Authenticated Encryption with Associated Data |
| AES | Chuẩn mã hóa nâng cao | Advanced Encryption Standard |
| CA | Tổ chức chứng thực | Certificate Authority |
| CNTT | Công nghệ thông tin | Information Technology |
| CBC | Chuỗi mật mã khối | Cipher Block Chaining |
| CRL | Danh sách các chứng thư bị thu hồi | Certificate Revocation List |
| DH | Thuật toán/phương pháp trao đổi khóa Diffie-Hellman | Diffie-Hellman |
| DSA | Thuật toán chữ ký số | Digital Signature Algorithm |
| ECDH | Diffie-Hellman dựa trên đường cong elliptic | Elliptic Curve Diffie Hellman |
| ECDSA | Thuật toán chữ ký số dựa trên đường cong elliptic | Elliptic Curve Digital Signature Algorithm |
| EEPROM | Bộ nhớ chỉ đọc có thể lập trình xóa điện | Electrically Erasable Programmable Read-Only Memory |
| FIPS | Các chuẩn xử lý thông tin liên bang | Federal Information Processing Standards |
| GCM | Chế độ đếm Galois | Galois Counter Mode |
| HMAC | Mã xác thực thông điệp hàm băm có khóa | Keyed-Hash Message Authentication Code |
| HTTPS | Giao thức truyền dẫn siêu văn bản an toàn | HyperText Transfer Protocol Secure |
| IP | Giao thức Internet | Internet Protocol |
| IPsec | Giao thức Internet an toàn | Internet Protocol Security |
| NIST | Viện tiêu chuẩn và công nghệ quốc gia (Hoa Kỳ) | National Institute of Standards and Technology |
| PP | Hồ sơ bảo vệ | Protection Profile |
| RBG | Bộ sinh bit ngẫu nhiên | Random Bit Generator |
| RSA | Thuật toán Rivest Shamir Adleman | Rivest Shamir Adleman Algorithm |
| SAR | Yêu cầu bảo đảm an toàn | Security Assurance Requirement |
| SD | Tài liệu hỗ trợ | Supporting Document |
| SFR | Yêu cầu chức năng an toàn | Security Functional Requirement |
| SHA | Thuật toán băm họ SHA | Secure Hash Algorithm |
| SSH | Vỏ bọc an toàn | Secure Shell |
| ST | Đích an toàn | Security Target |
| TLS | An toàn tầng giao vận | Transport Layer Security |
| TOE | Đích đánh giá | Target of Evaluation |
| TSF | Chức năng an toàn TOE | TOE Security Functionality |
| TSS | Đặc tả tóm tắt của TOE | TOE Summary Specification |
| VPN | Mạng riêng ảo | Virtual Private Network |

* 1. Giới thiệu Hồ sơ bảo vệ
     1. Tổng quan về TOE
     2. Tổng quan về tường lửa ứng dụng web

Tường lửa ứng dụng web hoặc WAF (sau đây gọi là 'TOE') được sử dụng để bảo vệ máy chủ web và ứng dụng web bằng cách phát hiện và ngăn chặn một cuộc tấn công bằng cách xác định tính quy phạm của yêu cầu người dùng HTTP và HTTPS lớp L7.

Chức năng chính của TOE là phát hiện và chặn luồng lưu lượng truy cập web độc hại vào máy chủ web và ứng dụng web theo chính sách bảo mật.

* + 1. Phạm vi và loại TOE

Định nghĩa của TOE trong Hồ sơ bảo vệ này là Tường lửa ứng dụng web phát hiện và ngăn chặn tấn công bằng cách xác định tính quy phạm của yêu cầu người dùng HTTP và HTTP lớp L7, được cung cấp dưới dạng thiết bị hoặc phần mềm. Bảng điều khiển quản lý có thể được bao gồm như một thành phần tùy chọn trong TOE, trong trường hợp này, nên được xác định là thành phần TOE trên tuyên bố về các mục tiêu an toàn của ST. Hồ sơ bảo vệ này xác định các yêu cầu bảo mật tối thiểu chung phải được cung cấp bởi TOE.

Các TOE nằm ngoài phạm vi của tiêu chuẩn này và dự kiến ​​sẽ được đưa vào trong phạm vi của phiên bản tiếp theo.

* + 1. Sử dụng TOE và các tính năng bảo mật chính

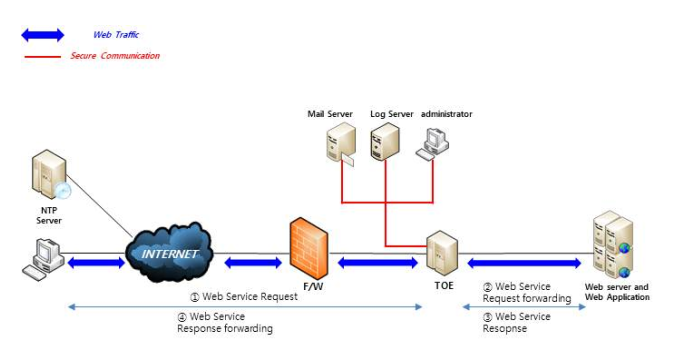
TOE được sử dụng cho mục đích phát hiện và ngăn chặn luồng lưu lượng truy cập web vào máy chủ web và ứng dụng web vi phạm các chính sách bảo mật do quản trị viên được ủy quyền thiết lập. TOE cung cấp chức năng phát hiện lưu lượng độc hại và ngăn chặn bằng cách so sánh lưu lượng truy cập web và luồng nội dung gói theo từng URL.

TOE cung cấp chức năng kiểm toán an toàn ghi lại các sự kiện chính dưới dạng dữ liệu kiểm toán khi chức năng an toàn và chức năng quản lý được vận hành; chức năng định danh và xác thực như xác minh danh tính của quản trị viên và xử lý lỗi xác thực; và chức năng bảo vệ TSF bao gồm bảo vệ dữ liệu được lưu trữ trong kho lưu trữ do TSF kiểm soát, tự kiểm tra TSF và xác minh tính toàn vẹn. Ngoài ra, nó bao gồm chức năng hỗ trợ mật mã như quản lý khóa mật mã và các hoạt động mật mã để hỗ trợ IPSec, TLS, SSH, HTTPS và các giao tiếp được mã hóa khác để quản trị viên quản lý giao tiếp truy cập; chức năng quản lý bảo mật để quản lý các chức năng bảo mật và thuộc tính bảo mật và định nghĩa về vai trò quản trị viên; và chức năng truy cập TOE để quản lý phiên truy cập của quản trị viên được ủy quyền.

* + 1. Môi trường hoạt động không phải TOE và TOE

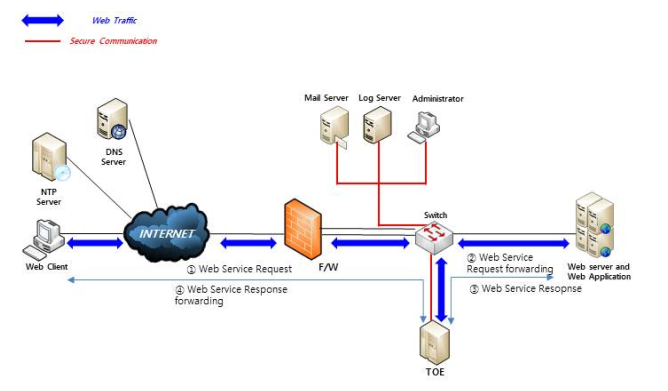
Môi trường hoạt động của TOE được xác định trong Hồ sơ bảo vệ này bao gồm loại 'In Line' hoặc 'Reverse Proxy', là loại mạng trong đó TOE trở thành điểm kết nối duy nhất.

[Hình 1] là một ví dụ về môi trường hoạt động chung của loại In Line. TOE được đặt ngay phía trước máy chủ web và ứng dụng web để phát hiện và chặn luồng lưu lượng truy cập web độc hại vào máy chủ web và ứng dụng web.



[Hình 1] Môi trường hoạt động của TOE(ví dụ: In Line type)

[Hình 2] là một ví dụ về môi trường hoạt động chung của kiểu Reverse Proxy, một trong những môi trường hoạt động đa dạng được áp dụng cho các trường hợp khó cài đặt vật lý In Line. TOE, được đặt ngay trước vùng web để hoạt động như một điểm kết nối duy nhất của máy chủ web và các ứng dụng web cần được bảo vệ, đặt địa chỉ IP của máy chủ web đã đăng ký trong DNS làm địa chỉ IP của TOE hoặc định cấu hình lưu lượng yêu cầu web được truyền từ máy khách web thông qua bộ chuyển đổi L4 để được gửi đến TOE.



[Hình 2] Môi trường hoạt động của TOE (ví dụ: Reverse Proxy type)

TOE được cài đặt và vận hành bên trong tổ chức được bảo vệ bởi Tường lửa, v.v. TOE được đặt trong môi trường vật lý an toàn, chỉ quản trị viên mới có thể truy cập được.

Quản trị viên được ủy quyền sẽ truy cập vào TOE thông qua trình duyệt web, giao tiếp nối tiếp và chương trình quản lý, v.v. và sẽ thực hiện quản lý bảo mật thông qua giao tiếp an toàn như IPSec, TLS, SSH và HTTPS.

Trong môi trường vận hành của TOE, có thể tồn tại các thực thể CNTT bên ngoài như máy chủ NTP để đồng bộ hóa thời gian, Máy chủ nhật ký để lưu trữ và quản lý dữ liệu kiểm toán, Máy chủ thư điện tử để thông báo cho quản trị viên được ủy quyền trong trường hợp mất dữ liệu kiểm toán, v.v. Người yêu cầu đánh giá của TOE tuân thủ Hồ sơ bảo vệ này sẽ xác định tất cả các thực thể CNTT bên ngoài tương tác với TOE trong ST.

Các thành phần khác như máy chủ NTP nằm ngoài TOE là môi trường vận hành TOE. Ngoài ra, những thành phần đó (ví dụ: các chức năng không liên quan gì đến các tính năng bảo mật của Tường lửa ứng dụng web) không liên quan đến các yêu cầu chức năng bảo mật (sau đây gọi là “SFR”) có thể được loại trừ khỏi phạm vi của TOE hoặc được phân loại thành non-TSF của TOE có xem xét phạm vi vật lý của TOE, v.v...

Hồ sơ bảo vệ này đã được phát triển có xem xét nhiều loại triển khai TOE khác nhau. Người yêu cầu đánh giá tuân thủ Hồ sơ bảo vệ này, sẽ mô tả mọi phần cứng, phần mềm hoặc phần sụn không phải TOE mà TOE yêu cầu để vận hành.

Người yêu cầu đánh giá phải có yêu cầu chức năng bảo mật bắt buộc có điều kiện được xác định trong Hồ sơ bảo vệ này, nếu các điều kiện sau được đáp ứng.

- Nếu TOE cung cấp các cơ chế xác thực và nhận dạng bổ sung (ví dụ: phương thức xác thực dựa trên chứng chỉ, phương thức OTP, v.v.) ngoài định danh và xác thực dựa trên ID/PW, FIA\_UAU.5 sẽ được đưa vào.

- Khi cung cấp các chức năng định danh và xác thực bổ sung, TOE có thể cung cấp các chức năng đó bằng cách nhận kết quả xác thực của các thực thể CNTT bên ngoài tương tác với TOE (ví dụ: thiết bị hỗ trợ 2FA tuân thủ các tiêu chuẩn FIDO) và theo đó FPT\_LEE.1(Extended ) sẽ được đưa vào thay vì FIA\_UAU.5. Trong trường hợp này, thông tin xác thực được sử dụng bởi các thực thể CNTT bên ngoài để thực hiện các phương pháp xác thực và nhận dạng bổ sung được quản lý an toàn bởi các thực thể CNTT bên ngoài, do đó, các mục tiêu bảo mật cho môi trường vận hành sẽ được bổ sung tương ứng.

- Trong trường hợp người dùng (quản trị viên được ủy quyền) truy cập trực tiếp vào máy chủ quản lý thông qua trình duyệt web hoặc chương trình truy cập đầu cuối, FTP\_TRP.1 sẽ được bao gồm. Giả sử rằng máy chủ web là môi trường vận hành TOE và nếu đường truyền thông an toàn được cung cấp thông qua giao tiếp giữa trình duyệt web của người dùng và máy chủ web, Người yêu cầu đánh giá sẽ thêm các mục tiêu bảo mật cho môi trường vận hành thay vì bao gồm FTP\_TRP.1. Và nếu trình duyệt web của người dùng truy cập máy chủ TOE thông qua máy chủ web, chẳng hạn như khi máy chủ web và máy chủ TOE được tách biệt về mặt vật lý để thực hiện giao tiếp, thì FTP\_TRP.1 được đưa vào để cung cấp đường dẫn an toàn giữa máy chủ TOE và người dùng, và FTP\_ITC.1 sẽ được đưa vào để cung cấp một kênh an toàn giữa máy chủ web và máy chủ TOE. FPT\_ITT.1 sẽ được bao gồm khi truyền dữ liệu TSF giữa các thành phần TOE được tách biệt về mặt vật lý. (ví dụ: Nếu giao tiếp giữa bảng điều khiển quản lý TOE và máy chủ quản lý được thực hiện trực tiếp, FPT\_ITT.1 sẽ được bao gồm)

- Khi TOE tương tác với các thực thể CNTT bên ngoài (ví dụ: máy chủ thư, máy chủ nhật ký, v.v.), FTP\_ITC.1 sẽ được đưa vào.

Người yêu cầu đánh giá sẽ bao gồm FAU\_STG.1, một yêu cầu chức năng an toàn bắt buộc có điều kiện, trong ST khi chức năng lưu trữ dấu vết kiểm toán được bảo vệ được triển khai trong TOE. Nếu chức năng không được triển khai trong TOE, chức năng đó phải được cung cấp trong môi trường vận hành (ví dụ: sử dụng DBMS, v.v.) và theo đó, các mục tiêu an toàn cho môi trường vận hành phải được thêm vào.

Người yêu cầu đánh giá sẽ bao gồm FPT\_STM.1, một yêu cầu chức năng an toàn tùy chọn, trong ST nếu TOE thực hiện một chức năng cung cấp tem thời gian đáng tin cậy. Nếu chức năng không được triển khai trong TOE, chức năng đó phải được cung cấp bởi môi trường vận hành (ví dụ: được cung cấp bởi hệ điều hành, v.v.) và theo đó, các mục tiêu an toàn cho môi trường vận hành phải được bổ sung.

Các yêu cầu chức năng an toàn tùy chọn có thể được triển khai tùy chọn trong TOE. Tuy nhiên, khi TOE cung cấp thêm các khả năng liên quan, Người yêu cầu đánh giá phải bao gồm các SFR tương ứng. Người yêu cầu đánh giá phải chú ý không bỏ qua các yêu cầu chức năng an toàn cho các tính năng an toàn do TOE cung cấp bằng cách tham khảo các lưu ý ứng dụng khi áp dụng từng yêu cầu chức năng an toàn tùy chọn liên quan đến khả năng áp dụng của các yêu cầu chức năng an toàn tùy chọn.

* + 1. Quy ước

Ký hiệu, định dạng và quy ước được sử dụng trong PP này nhất quán với Tiêu chí chung để Đánh giá An toàn công nghệ thông tin.

CC cho phép thực hiện một số thao tác đối với các yêu cầu chức năng: lặp lại, gán, lựa chọn và sàng lọc. Mỗi thao tác được sử dụng trong PP này.

**Lặp lại**

Lặp lại được sử dụng khi một thành phần được lặp lại với các hoạt động khác nhau. Kết quả của phép lặp được đánh dấu bằng số lần lặp trong ngoặc đơn sau mã định danh thành phần, tức là, được biểu thị là (Số lần lặp).

**Lựa chọn**

Điều này được sử dụng để chọn một hoặc nhiều tùy chọn do CC cung cấp khi nêu yêu cầu. Kết quả lựa chọn được hiển thị dưới dạng gạch chân và in nghiêng.

**Sàng lọc**

Điều này được sử dụng để thêm chi tiết và do đó hạn chế hơn nữa một yêu cầu. Kết quả của sự sàng lọc được thể hiện bằng văn bản in đậm.

**Đích an toàn (ST)**

Điều này được sử dụng để đại diện cho quyết định cuối cùng của các thuộc tính được thực hiện bởi Người yêu cầu đánh giá. Hoạt động của Người yêu cầu đánh giá được biểu thị trong dấu ngoặc nhọn, như trong { quyết định bởi Người yêu cầu đánh giá }. Ngoài ra, các hoạt động của SFR không được hoàn thành trong Hồ sơ bảo vệ phải được hoàn thành bởi Người yêu cầu đánh giá.

“Lưu ý áp dụng” được cung cấp để làm rõ mục đích của các yêu cầu, cung cấp thông tin cho các mục tùy chọn trong quá trình triển khai và xác định tiêu chí "Đạt/Không đạt" cho một yêu cầu. Các Lưu ý áp dụngđược cung cấp với các yêu cầu tương ứng nếu cần thiết.

* 1. Các yêu cầu tuân thủ

1. Yêu cầu tuân thủ CC

|  |  |  |
| --- | --- | --- |
| CC | | Tiêu chí chung để đánh giá an toàn công nghệ thông tin, Phiên bản 3.1, Sửa đổi 5   * TCVN 8709-1:2011 Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 1: Giới thiệu và mô hình tổng quát. * TCVN 8709-2:2011 Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 2: Các thành phần chức năng an toàn. * TCVN 8709-3:2011 Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 3: Các thành phần đảm bảo an toàn. |
| Yêu cầu tuân thủ | Phần 2 Các thành phần chức năng bảo mật | Mở rộng: FDP\_EDI.1, FMT\_PWD.1, FPT\_LEE.1, FPT\_PST.1, FPT\_TUD.1 |
| Phần 3 Các thành phần đảm bảo an toàn | *Phù hợp* |
| Gói | Đã tăng cường : *Đã tăng cường* EAL1 (ATE\_FUN.1) |

1. Yêu cầu tuân thủ PP

Hồ sơ bảo vệ này không yêu cầu tuân thủ các PP khác.

1. Yêu cầu tuân thủ gói

Hồ sơ bảo vệ này yêu cầu tuân thủ gói đảm bảo EAL1 được tăng cường bằng ATE\_FUN.1.

1. Cơ sở yêu cầu tuân thủ

Vì Hồ sơ bảo vệ này không yêu cầu tuân thủ với các Hồ sơ bảo vệ khác, nên không cần thiết phải mô tả cơ sở lý luận của yêu cầu tuân thủ

1. Tuyên bố tuân thủ PP

Hồ sơ bảo vệ này yêu cầu “tuân thủ PP nghiêm ngặt” của bất kỳ ST hoặc PP nào yêu cầu tuân thủ PP này.

* 1. Các mục tiêu an toàn

7.1 Các mục tiêu an toàn cho môi trường hoạt động

OE.LOG\_BACKUP

Quản trị viên được ủy quyền định kỳ kiểm tra dung lượng lưu trữ dữ liệu kiểm tra dự phòng trong trường hợp mất dữ liệu kiểm tra và tiến hành sao lưu dữ liệu kiểm tra (máy chủ nhật ký bên ngoài hoặc thiết bị lưu trữ riêng, v.v.) để ngăn chặn mất dữ liệu kiểm toán.

OE.PHYSICAL\_CONTROL

TOE phải được đặt trong môi trường an toàn về mặt vật lý mà chỉ quản trị viên được ủy quyền mới được phép truy cập và các phương tiện bảo vệ được cung cấp.

OE.SECURITY\_MAINTENANCE

Khi môi trường mạng bên trong thay đổi do thay đổi cấu hình mạng, tăng/giảm Máy chủ Web và tăng/giảm Ứng dụng Web, v.v., các chính sách bảo mật và môi trường thay đổi phải được phản ánh ngay lập tức với các chính sách vận hành TOE trong để duy trì cùng một mức độ an toàn như trước đây.

OE.TRUSTED\_ADMIN Quản trị viên được ủy quyền của TOE phải là người dùng không độc hại, đã được đào tạo thích hợp cho các chức năng quản lý TOE và hoàn thành chính xác các nhiệm vụ theo hướng dẫn của quản trị viên.

OE.OPERATION\_SYSTEM\_REINFORCEMENT

Quản trị viên được ủy quyền của TOE sẽ đảm bảo độ tin cậy và bảo mật của hệ điều hành bằng cách thực hiện củng cố các lỗ hổng mới nhất của hệ điều hành mà TOE được cài đặt và vận hành.

|  |
| --- |
| Lưu ý áp dụng  Do thành phần TOE có thể không sử dụng một hệ điều hành độc lập theo phương pháp thực hiện TOE (khi bảng điều khiển quản lý được bao gồm trong thành phần TOE), quản trị viên được ủy quyền nên cẩn thận rằng cài đặt hệ điều hành của thực thể CNTT bên ngoài hoạt động trong cùng một hệ điều hành không ảnh hưởng đến hoạt động an toàn của TOE. |

OE.SINGLE\_POINT\_OF\_CONNECTION

Kết nối với máy chủ web hoặc ứng dụng web chỉ nên được truy cập thông qua TOE.

|  |
| --- |
| Lưu ý áp dụng  Trong trường hợp loại Reverse Proxy, TOE được cài đặt bằng cách kết nối với bộ chuyển mạch và hoạt động như điểm kết nối duy nhất với ứng dụng web, nên được thiết lập để đảm bảo rằng yêu cầu truy cập web của người dùng vượt qua TOE bằng cách chuyển đổi địa chỉ IP của máy chủ web và ứng dụng web đã đăng ký DNS. |

Các yêu cầu chức năng an toàn

Các yêu cầu an toàn xác định các yêu cầu chức năng an toàn và các yêu cầu đảm bảo phải được đáp ứng bởi TOE Yêu cầu tuân thủ PP này.

Các yêu cầu chức năng an toàn có trong PP này được lấy từ CC Phần 2 và Định nghĩa thành phần mở rộng của Phụ lục.

Ngoài ra, các yêu cầu chức năng an toàn được phân loại thành SFR bắt buộc, SFR bắt buộc có điều kiện và SFR tùy chọn, như sau:

• Các SFR bắt buộc: được yêu cầu triển khai bắt buộc trong ‘Tường lửa ứng dụng web’

• Các SFR bắt buộc có điều kiện: bắt buộc phải triển khai nếu các điều kiện đã nêu được đáp ứng.

• Các SFR tùy chọn: không bắt buộc phải triển khai bắt buộc trong ‘Tường lửa ứng dụng web’. Tuy nhiên, khi TOE cung cấp thêm các khả năng liên quan, Người yêu cầu đánh giá phải bao gồm các SFR tương ứng.

Bảng sau đây tóm tắt các yêu cầu chức năng bảo mật được sử dụng trong PP:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lớp chức năng an toàn** | **Thành phần chức năng an toàn** | | **Ghi chú** |
| FAU | FAU\_ARP.1 | Cảnh báo an toàn | SFR bắt buộc |
| FAU\_GEN.1 | Tạo dữ liệu kiểm toán | SFR bắt buộc |
| FAU\_SAA.1 | Phân tích vi phạm tiềm năng | SFR bắt buộc |
| FAU\_SAR.1 | Đánh giá kiểm toán | SFR bắt buộc |
| FAU\_SAR.3 | Đánh giá kiểm toán có thể lựa chọn | SFR bắt buộc |
| FAU\_STG.1 | Lưu trữ dấu vết kiểm toán được bảo vệ | SFR bắt buộc có điều kiện |
| FAU\_STG.3 | Hành động trong trường hợp có thể mất dữ liệu kiểm toán | SFR bắt buộc có điều kiện |
| FAU\_STG.4 | Ngăn ngừa mất dữ liệu kiểm toán | SFR bắt buộc có điều kiện |
| FCS | FCS\_CKM.1 | Tạo khóa mật mã | Bắt buộc SFR |
| FCS\_CKM.2 | Phân phối khóa mật mã | SFR tùy chọn |
| FCS\_CKM.4 | Phá hủy khóa mật mã | SFR bắt buộc |
| FCS\_COP.1 | Hoạt động mật mã | SFR bắt buộc |
| FCS\_RGB.1  (Mở rộng) | Tạo bit ngẫu nhiên | SFR bắt buộc |
| FDP | FDP\_IFC.1 | Kiểm soát luồng thông tin tập hợp con | SFR bắt buộc |
| FDP\_IFF.1 | Thuộc tính an toàn đơn giản | SFR bắt buộc |
| FDP\_ED1.1  (Mở rộng) | Hành động phản hồi và xác minh tính toàn vẹn của dữ liệu được lưu trữ bên ngoài | SFR bắt buộc |
| FIA | FIA\_AFL.1 | Xử lý lỗi xác thực | SFR bắt buộc |
| FIA\_SOS.1 | Xác minh bí mật | SFR bắt buộc |
| FIA\_UAU.1 | Thời gian xác thực | SFR bắt buộc |
| FIA\_UAU.4 | Cơ chế xác thực sử dụng một lần | SFR bắt buộc |
| FIA\_UAU.5 | Nhiều cơ chế xác thực | SFR bắt buộc có điều kiện |
| FIA\_UAU.7 | Phản hồi xác thực được bảo vệ | SFR bắt buộc |
| FIA\_UID.1 | Thời gian nhận dạng | SFR bắt buộc |
| FMT | FMT\_MOF.1 | Quản lý hành vi chức năng bảo mật | SFR bắt buộc |
| FMT\_MSA.1 | Quản lý thuộc tính an toàn | SFR bắt buộc |
| FMT\_MSA.3 | Khởi tạo thuộc tính tĩnh | SFR bắt buộc |
| FMT\_MTD.1 | Quản lý dữ liệu TSF | SFR bắt buộc |
| FMT\_PWD.1(Mở rộng) | Quản lý ID và mật khẩu | SFR bắt buộc |
| FMT\_SMF .1 | Đặc tả chức năng quản lý | SFR bắt buộc |
| FMT\_SMR.1 | Vai trò an toàn | SFR bắt buộc |
| FPT | FPT\_ITT.1 | Bảo vệ truyền dữ liệu TSF nội bộ cơ bản | SFR bắt buộc có điều kiện |
| FPT\_LEE.1(Mở rộng) | Các thực thể bên ngoài có thể liên kết – xác thực | SFR bắt buộc có điều kiện |
| FPT\_PST.1(Mở rộng) | Bảo vệ cơ bản dữ liệu TSF được lưu trữ | SFR bắt buộc |
| FPT\_RCV.2 | Phục hồi tự động | SFR bắt buộc |
| FPT\_STM.1 | Dấu thời gian đáng tin cậy | SFR tùy chọn |
| FPT\_TST.1 | Thử nghiệm TSF | SFR bắt buộc |
| FPT\_TUD.1(Mở rộng) | Cập nhật bản vá bảo mật TSF | SFR bắt buộc |
| FTA | FTA\_SSL.1 | Khóa phiên do TSF khởi tạo | SFR bắt buộc có điều kiện |
| FTA\_SSL.3 | Kết thúc do TSF khởi xướng | SFR bắt buộc có điều kiện |
| FTA\_TSE.1(1) | Thiết lập phiên TOE | SFR bắt buộc |
| FTA\_TSE.1(2) | Thiết lập phiên TOE | SFR bắt buộc có điều kiện |
| FTP | FTP\_ITC.1 | Kênh tin cậy liên TSF | SFR bắt buộc có điều kiện |
| FTP\_TRP.1 | Đường dẫn tin cậy | SFR bắt buộc có điều kiện |

[Bảng 1] Các yêu cầu chức năng an toàn

Yêu cầu chức năng an toàn (SFR bắt buộc)

WAF yêu cầu tuân thủ PP này phải đáp ứng các SFR bắt buộc sau đây:

|  |  |  |
| --- | --- | --- |
| **Lớp chức năng an toàn** | **Thành phần chức năng an toàn** | |
| FAU | FAU\_ARP.1 | Cảnh báo an toàn |
| FAU\_GEN.1 | Tạo dữ liệu kiểm toán |
| FAU\_SAA.1 | Phân tích vi phạm tiềm năng |
| FAU\_SAR.1 | Đánh giá kiểm toán |
| FAU\_SAR.3 | Đánh giá kiểm toán có thể lựa chọn |
| FCS | FCS\_CKM.1 | Tạo khóa mật mã |
| FCS\_CKM.4 | Phá hủy khóa mật mã |
| FCS\_COP.1 | Hoạt động mật mã |
| FCS\_RBG.1(Extended) | Tạo bit ngẫu nhiên |
| FDP | FDP\_IFC.1 | Kiểm soát luồng thông tin tập hợp con |
| FDP\_IFF.1 | Thuộc tính an toàn đơn giản |
| FDP\_EDI.1(Extended) | Hành động phản hồi và xác minh tính toàn vẹn của dữ liệu được lưu trữ bên ngoài |
| FIA | FIA\_AFL.1 | Xử lý lỗi xác thực |
| FIA\_SOS.1 | Xác minh bí mật |
| FIA\_UAU.1 | Thời gian xác thực |
| FIA\_UAU.4 | Cơ chế xác thực sử dụng một lần |
| FIA\_UAU.7 | Phản hồi xác thực được bảo vệ |
| FIA\_UID.1 | Thời gian định danh |
| FMT | FMT\_MOF.1 | Quản lý hành vi chức năng bảo mật |
| FMT\_MSA.1 | Quản lý thuộc tính an toàn |
| FMT\_MSA.3 | Khởi tạo thuộc tính tĩnh |
| FMT\_MTD.1 | Quản lý dữ liệu TSF |
| FMT\_PWD.1(Extended) | Quản lý ID và mật khẩu |
| FMT\_SMF.1 | Đặc tả chức năng quản lý |
| FMT\_SMR.1 | Vai trò an toàn |
| FPT | FPT\_PST.1(Extended) | Bảo vệ truyền dữ liệu TSF nội bộ cơ bản |
| FPT\_RCV.2 | Phục hồi tự động |
| FPT\_TST.1 | Thử nghiệm TSF |
| FPT\_TUD.1(Extended) | Cập nhật bản vá bảo mật TSF |
| FTA | FTA\_MCS.2 | Giới hạn thuộc tính trên từng người dùng theo các phiên đồng thời |
| FTA\_TSE.1(1) | Thiết lập phiên TOE |

[Bảng 2] Các yêu cầu chức năng an toàn bắt buộc

Kiểm toán an toàn (FAU)

1. FAU\_ARP.1 Cảnh báo an toàn

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | FAU\_SAA.1 Phân tích vi phạm tiềm năng. |
| FAU\_ARP.1.1 | TSF sẽ thực hiện [lựa chọn: *danh sách các hành động*] khi phát hiện một vi phạm an toàn tiềm ẩn |

|  |
| --- |
| Lưu ý áp dụng   * Nếu kết quả tự kiểm tra TOE không thành công, các chức năng phản hồi sẽ được thực hiện.   - Ví dụ về các chức năng phản hồi sẽ được thực hiện khi kết quả tự kiểm tra bị lỗi như sau:  • *Gián đoạn thực thi chương trình, hiển thị màn hình thông báo cảnh báo, khởi động lại quy trình, v.v.*   * Nếu kết quả xác minh tính toàn vẹn của TOE là lỗi, các chức năng phản hồi sẽ được thực hiện.   - Ví dụ về các chức năng phản hồi sẽ được thực hiện khi kết quả xác minh tính toàn vẹn bị lỗi như sau:  • *Gián đoạn thực thi chương trình, hiển thị màn hình thông báo cảnh báo, v.v.* |

1. FAU\_GEN.1 Tạo dữ liệu kiểm tra

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | FPT\_STM.1 Dấu thời gian đáng tin cậy |
| FAU\_GEN.1.1 | TSF phải có khả năng tạo ra một bản ghi kiểm tra các sự kiện có thể kiểm toán sau:  a) Khởi động và tắt các chức năng kiểm toán  b) Tất cả các sự kiện có thể đánh giá đối với cấp độ đánh giá không xác định; và  c) [lựa chọn: *các sự kiện có thể kiểm tra được xác định cụ thể khác* ] |
| FAU\_GEN.1.2 | TSF phải ghi lại trong mỗi bản ghi kiểm tra ít nhất các thông tin sau: a) Ngày và thời gian của sự kiện, loại sự kiện, nhận dạng chủ thể (nếu có), và kết quả (thành công hay thất bại) của sự kiện; và  b) Đối với mỗi loại sự kiện đánh giá, dựa trên định nghĩa sự kiện có thể đánh giá của các thành phần chức năng có trong PP/ST, [lựa chọn: *thông tin liên quan đến đánh giá khác*] |

|  |
| --- |
| Lưu ý áp dụng   * TOE sẽ tạo hồ sơ kiểm toán cho các sự kiện kiểm toán chính.   - [Bảng 3] bên dưới hiển thị các sự kiện kiểm tra mà hồ sơ kiểm tra phải được tạo |

|  |  |  |
| --- | --- | --- |
| Danh mục phụ | Sự kiện kiểm toán | Thông tin kiểm toán viên bổ sung |
| Định danh và xác thực | Đăng nhập và đăng xuất của người dùng |  |
| Đăng ký, thay đổi, xóa người dùng |  |
| Đạt đến ngưỡng xác thực người dùng không thành công và các hành động đã thực hiện |  |
| Tất cả thay đổi mật khẩu |  |
| Quản lý an toàn | Đăng ký, xóa, thay đổi địa chỉ IP của các thiết bị đầu cuối quản lý |  |
| Thực thi chức năng quản lý bảo mật và tất cả các thay đổi và xóa các giá trị thuộc tính bảo mật.  \*\* Tuy nhiên, trong số các chức năng quản lý bảo mật, các chức năng 'Truy vấn hồ sơ kiểm toán' và 'Truy vấn thông tin phiên bản TOE' bị loại trừ | Thay đổi dữ liệu thuộc tính bảo mật |
| Tài khoản mặc định (ID)/Mật khẩu thay đổi |  |
| Chặn IP truy cập thiết bị đầu cuối quản lý |  |
| Quản lý phiên đáng tin cậy | Khóa hoặc chấm dứt phiên của người dùng |  |
| Hành động phản hồi khi phát hiện các lần đăng nhập trùng lặp của cùng một tài khoản |  |
| Từ chối các phiên mới dựa trên giới hạn về số lượng phiên đồng thời |  |
| Tạo khóa mật mã | Lỗi tạo khóa mật mã |  |
| Hoạt động mật mã | Lỗi hoạt động mật mã (bao gồm loại hoạt động mật mã) |  |
| Bản ghi kiểm toán | Khởi động và tắt các chức năng kiểm toán TOE ở dạng thiết bị H/W |  |

[Bảng 3] Các sự kiện kiểm toán chính cần được ghi lại một cách bắt buộc.

- [Bảng 4] bên dưới hiển thị các sự kiện kiểm tra mà các bản ghi kiểm tra có thể được tạo khi cung cấp một chức năng

|  |  |  |
| --- | --- | --- |
| Danh mục phụ | Sự kiện kiểm toán | Thông tin kiểm toán bổ sung |
| Tự bảo vệ | Thực hiện tự kiểm tra | chức năng bảo mật với tự kiểm tra không thành công |
| Thực hiện xác minh tính toàn vẹn của chính TOE | Các thành phần với xác minh không toàn vẹn |
| Cập nhật bảo vệ | Xác minh tính hợp lệ của tệp được cập nhật bởi quản trị viên |  |
| Cập nhật  Bảo vệ |  |
| Hồ sơ kiểm toán | Thực hiện xác minh tính hợp lệ của tệp cập nhật Hồ sơ kiểm tra Khởi động và tắt chức năng kiểm tra TOE dưới dạng phần mềm |  |
| Khởi động và tắt chức năng kiểm toán TOE dưới dạng phần mềm |  |
| Quản lý an toàn | hồ sơ kiểm toán |  |

[Bảng 4] Các sự kiện kiểm tra phải được ghi lại khi cung cấp chức năng

* Nếu TOE phát hiện nỗ lực sử dụng lại thông tin xác thực bị cấm sử dụng lại, xác thực sẽ không thành công và một bản ghi kiểm toán về sự kiện lỗi xác thực sẽ được tạo.
* Hồ sơ đánh giá sẽ được tạo ra cho các kết quả tự kiểm tra.
* Nội dung và kết quả xác minh tính toàn vẹn sẽ được xác nhận thông qua *màn hình hiển thị, hồ sơ kiểm toán.*
* Hồ sơ kiểm tra sẽ được tạo ra cho kết quả xác minh tính toàn vẹn.
* Cập nhật kết quả xác nhận tệp (thành công • thất bại) sẽ được ghi lại trong hồ sơ kiểm toán.
* Hồ sơ kiểm tra sẽ được tạo cho kết quả cài đặt bản cập nhật và lý do thất bại.
* Hồ sơ kiểm tra sẽ được tạo khi chức năng khóa hoặc chấm dứt phiên được kích hoạt.
* Hồ sơ kiểm toán sẽ được tạo khi chặn truy cập trùng lặp.
* Hồ sơ kiểm toán không được chứa nhiều thông tin hơn mức cần thiết.

- Các nội dung ít nhất phải có trong hồ sơ kiểm toán như sau.

• Ngày và giờ của sự kiện, loại sự kiện, danh tính của đối tượng gây ra sự kiện (ví dụ: *tài khoản, quy trình, IP*, v.v.) và kết quả của sự kiện (thành công • thất bại)

- Thông tin như vậy vì thông tin xác thực (ví dụ: *mật khẩu*, v.v.) và khóa mã hóa sẽ không được lưu trữ trong hồ sơ kiểm toán

* Dữ liệu nhạy cảm (ví dụ: *mật khẩu, số đăng ký cư trú*, v.v.) sẽ không được ghi lại hoặc sẽ được tạo ra bằng cách xử lý bằng mặt nạ nếu việc ghi lại là không thể tránh khỏi.
* Mỗi thành phần của TOE sẽ tạo hồ sơ kiểm tra bằng cách sử dụng thông tin thời gian đáng tin cậy.

- Thông tin về thời gian đáng tin cậy nên sử dụng thông tin về thời gian do máy chủ NTP hoặc hệ điều hành cung cấp.

* Nếu WAS (Tomcat, Jesus, v.v.) được bao gồm trong gói TOE, TOE sẽ được triển khai sao cho thông tin quan trọng không được bao gồm trong nhật ký WAS.

- Nó có thể được triển khai sao cho chỉ có thể để lại nhật ký trong lưu trữ hồ sơ kiểm toán của TOE mà không rời khỏi nhật ký WAS.

- Thông tin quan trọng như mật khẩu và khóa mã hóa sẽ không được để lại ở dạng văn bản thuần túy trong nhật ký WAS.

* TOE sẽ tạo hồ sơ kiểm toán cho các sự kiện kiểm toán chính.

- TOE sẽ tạo các bản ghi kiểm toán cho lưu lượng web được phép và bị chặn bởi TOE.

• Bao gồm kết quả cho phép và chặn lưu lượng truy cập web theo FDP\_IFF.1.

- Có thể hỏi các sự kiện xảy ra trong một khoảng thời gian cụ thể và tổng lượng lưu lượng bị chặn.

- Các bản ghi kiểm tra sẽ được tạo cho các hành động quản lý bảo mật liên quan đến các quy tắc chặn và phát hiện lưu lượng truy cập web do quản trị viên thực hiện trong lớp FMT.

- Hồ sơ kiểm tra ít nhất phải bao gồm ngày và thời gian của sự kiện, loại sự kiện, danh tính của đối tượng gây ra sự kiện và kết quả của sự kiện.

1. FAU\_SAA.1 Phân tích vi phạm tiềm ẩn

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | FAU\_GEN.1 Tạo dữ liệu kiểm tra |
| FAU\_SAA.1.1 | TSF sẽ có thể áp dụng một bộ quy tắc trong việc giám sát các sự kiện được kiểm toán và dựa trên các quy tắc này chỉ ra một vi phạm tiềm ẩn đối với việc thực thi các SFR. |
| FAU\_SAA.1.2 | TSF sẽ thực thi các quy tắc sau để giám sát các sự kiện được kiểm toán:  a) Tích lũy hoặc kết hợp của [lựa chọn: *tập hợp con của các sự kiện có thể kiểm toán được xác định*] đã biết để chỉ ra một vi phạm an toàn tiềm ẩn  b) [lựa chọn: *bất kỳ quy tắc nào khác*] |

|  |
| --- |
| Lưu ý áp dụng   * Nếu kết quả tự kiểm tra của TOE không thành công, chức năng phản hồi sẽ được thực hiện. * TOE sẽ thực hiện chức năng phản hồi nếu xác minh tính toàn vẹn không thành công. |

1. FAU\_SAR.1 Đánh giá kiểm tra

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | FAU\_GEN.1 Tạo dữ liệu kiểm tra |
| FAU\_SAR.1.1 | TSF sẽ cung cấp cho [quản trị viên được ủy quyền] khả năng đọc [tất cả dữ liệu kiểm tra] từ các bản ghi kiểm tra. |
| FAU\_SAR.1.2 | TSF phải cung cấp các bản ghi kiểm tra theo cách thức phù hợp để quản trị viên được ủy quyền diễn giải thông tin |

|  |
| --- |
| Lưu ý áp dụng   * TOE sẽ cung cấp một chức năng cho quản trị viên được ủy quyền để truy vấn hồ sơ kiểm toán.   - Hồ sơ kiểm định chỉ được truy vấn thông qua chức năng bảo mật do TOE cung cấp.  - TOE phải cung cấp hồ sơ kiểm toán cho quản trị viên được ủy quyền để giải thích đúng thông tin. |

1. FAU\_SAR.3 Đánh giá kiểm tra có thể lựa chọn

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | FAU\_SAR.1 Đánh giá kiểm toán |
| FAU\_SAR.3.1 | TSF sẽ cung cấp khả năng áp dụng [lựa chọn: *phương pháp lựa chọn và/hoặc sắp xếp*] dữ liệu kiểm toán dựa trên [lựa chọn: *tiêu chí có quan hệ logic*] |

|  |
| --- |
| Các lưu ý của ứng dụng   * TOE sẽ cung cấp chức năng cho người quản trị để chọn một điều kiện logic khi truy vấn các bản ghi kiểm toán và để tìm kiếm hoặc sắp xếp các bản ghi theo các điều kiện khác nhau. * Có thể truy vấn các sự kiện xảy ra trong một khoảng thời gian cụ thể và tổng lưu lượng bị chặn. |

Hỗ trợ mật mã (FCS)

1. FCS\_CKM.1 Tạo khóa mật mã

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | [FCS\_CKM.2 Phân phối khóa mật mã, hoặc FCS\_COP.1 Hoạt động mật mã]  FCS\_CKM.4 Phá hủy khóa mật mã |
| FCS\_CKM.1.1 | TSF sẽ tạo khóa mật mã theo thuật toán tạo khóa mật mã được lựa chọn [lựa chọn: *thuật toán tạo khóa mật mã*] và được lựa chọn kích thước khóa mật mã [lựa chọn: *kích thước khóa mật mã*] đáp ứng những điều sau: [lựa chọn*: danh sách tiêu chuẩn*] |

|  |
| --- |
| Lưu ý áp dụng   * TOE sẽ tạo các khóa mật mã theo một phương pháp an toàn.   - Ví dụ về các phương pháp tạo khóa mật mã an toàn như sau:  • *Dẫn xuất khóa dựa trên mật khẩu (PKCS#5 v2.1(RFC 8018), NIST SP 800-132, v.v.)*  *• Dẫn xuất khóa với các khóa chia sẻ trước (TTAK. KO-12.0272)*  *• Tạo khóa sử dụng trình tạo bit ngẫu nhiên (CTR\_DRBG, HASH DRBG, HMAC\_DRBG, v.v.)*  - Trình tạo bit ngẫu nhiên sẽ được triển khai tuân thủ các tiêu chuẩn trong và ngoài nước.  - Có thể tạo các cặp khóa bất đối xứng (khóa chung/khóa riêng) hoặc khóa đối xứng bằng cách sử dụng các bit ngẫu nhiên được tạo bởi trình tạo bit ngẫu nhiên.  - Chỉ được sử dụng chức năng tạo khóa dựa trên mật khẩu để tạo Khóa mã hóa khóa (KEK).  • Khóa mã hóa khóa ban đầu sẽ được tạo khác nhau cho mỗi TOE.  • Dữ liệu ban đầu cần thiết để tạo khóa mã hóa khóa có thể được nhập trực tiếp hoặc đưa vào từ các giá trị được lưu trữ trong phương tiện lưu trữ như thẻ thông minh, USB bảo mật, mã thông báo bảo mật (HSM: Mô-đun bảo mật phần cứng).  • Nên sử dụng các sản phẩm đã đạt được báo cáo kiểm tra chức năng bảo mật hoặc chứng chỉ CC trong nước/nước ngoài cho phương tiện lưu trữ.  • Để biết chi tiết, tham khảo phần Tạo khóa mã hóa của ‘Hướng dẫn quản lý khóa mã hóa’ (Bộ Khoa học và CNTT-TT, 2014).  • Nếu mật khẩu được sử dụng làm dữ liệu ban đầu để tạo khóa mã hóa khóa (KEK), giá trị được nhập tại thời điểm cài đặt ban đầu của sản phẩm có thể được lưu trữ và sử dụng, đồng thời dữ liệu được lưu trữ sẽ được bảo vệ khỏi các nỗ lực tiếp xúc trái phép . |

1. CKM.4 Phá hủy khóa mật mã

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | [FDP\_ITC.1 Nhập dữ liệu người dùng không có thuộc tính bảo mật hoặc FDP\_ITC.2 Nhập dữ liệu người dùng có thuộc tính bảo mật hoặc FCS\_CKM.1 Tạo khóa mật mã] |
| FCS\_CKM.4.1 | TSF sẽ hủy khóa mật mã theo quy trình hủy khóa mật mã được lựa chọn phương pháp [lựa chọn: *phương pháp hủy khóa mật mã*] đáp ứng những điều sau: [lựa chọn: *danh sách các tiêu chuẩn*]. |

|  |
| --- |
| Lưu ý áp dụng   * TOE sẽ hủy một cách an toàn các khóa mật mã được tạo hoặc sử dụng trong TOE.   - △Khi chấm dứt thực thi TOE, △Khi gọi chức năng xóa khóa mật mã, △Khi chấm dứt giao tiếp mật mã, v.v., tất cả các khóa mật mã và thông tin liên quan đến khóa mật mã đã hết hạn sẽ bị hủy.  - Khi hủy khóa mật mã có thể sử dụng phương pháp ghi đè ít nhất 3 lần với các giá trị 0 hoặc 1.  - Chi tiết tham khảo phương pháp hủy khóa mật mã trong ‘Hướng dẫn quản lý khóa mật mã’ (Bộ KH&CN, 2014). |

1. FCS\_COP.1 Hoạt động mật mã

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | [FDP\_ITC.1 Nhập dữ liệu người dùng không có thuộc tính bảo mật hoặc FDP\_ITC.2 Nhập dữ liệu người dùng có thuộc tính bảo mật hoặc FCS\_CKM.1 Tạo khóa mật mã] FCS\_CKM.4 Phá hủy khóa mật mã |
| FCS\_COP.1.1 | TSF sẽ thực hiện [lựa chọn: *danh sách của các hoạt động mật mã*] phù hợp với một thuật toán mã hóa được lựa chọn [lựa chọn: *thuật toán mã hóa*] và kích thước khóa mật mã [lựa chọn: *kích thước khóa mật mã*] đáp ứng những điều sau: [lựa chọn: *danh sách các tiêu chuẩn*]. |

|  |
| --- |
| Lưu ý áp dụng   * TOE sẽ sử dụng thuật toán mã hóa được đề xuất khi truyền và lưu trữ thông tin quan trọng. * Thuật toán mã hóa được đề xuất là thuật toán tiêu chuẩn có cường độ bảo mật từ 112 bit trở lên. Tham khảo [Đính kèm] tài liệu phụ trợ. Ví dụ như sau:   - Thuật toán hàm băm: SHA-224 trở lên  - Thuật toán khóa đối xứng: Độ dài khóa 128 bit trở lên  - Thuật toán khóa công khai: RSA 2048 trở lên, DSA(2018, 224) trở lên  - Thuật toán chữ ký số: RSA- PSS 2048 trở lên, KCDSA(2048, 224) trở lên, ECDSA/EC-KCDSA (B-233, B-283, K-223, K-283, P-224, P-256)   * Tuy nhiên, việc sử dụng TDES (bao gồm 2 phím và 3 phím) không được phép. * Khi sử dụng mật mã khối, chế độ ECB sẽ không được sử dụng nếu kích thước văn bản thuần túy lớn hơn kích thước khối mã hóa. * Khi sử dụng mật mã khối, IV cố định sẽ không được sử dụng ở chế độ CFB hoặc OFB. * Sử dụng các thuật toán mật mã tiêu chuẩn trong nước/nước ngoài và khuyến nghị sử dụng thuật toán mật mã quốc gia. * Để biết chi tiết về thuật toán mật mã có độ bền bảo mật từ 112 bit trở lên, hãy tham khảo 'Hướng dẫn về thuật toán mật mã và độ dài khóa' (Bộ Khoa học và CNTT, 2018), 'Tiêu chuẩn xác thực mô-đun mật mã phần mềm' và 'NIST SP 800- 131Ar2'. |

1. FCS\_RBG.1 Tạo bit ngẫu nhiên (Mở rộng)

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| FCS\_RBG.1.1 | TSF sẽ tạo bit ngẫu nhiên bằng cách sử dụng bộ tạo bit ngẫu nhiên được lựa chọn đáp ứng [lựa chọn: danh sách các tiêu chuẩn] sau đây. |

|  |
| --- |
| Lưu ý áp dụng   * Ví dụ về các phương pháp tạo khóa mật mã an toàn như sau:   *• Dẫn xuất khóa dựa trên mật khẩu (PKCS#5 v2.1(RFC 8018), NIST SP 800-132, v.v.)*  *• Dẫn xuất khóa với các khóa chia sẻ trước*  *• Tạo khóa bằng cách sử dụng trình tạo bit ngẫu nhiên (CTR\_DRBG, HASH DRBG, HMAC\_DRBG, v.v.)*   * Trình tạo bit ngẫu nhiên sẽ được triển khai tuân thủ các tiêu chuẩn trong và ngoài nước. * Có thể tạo các cặp khóa bất đối xứng (khóa chung/khóa riêng) hoặc khóa đối xứng bằng cách sử dụng các bit ngẫu nhiên do trình tạo bit ngẫu nhiên tạo ra. * Mật khẩu người dùng được TOE sử dụng để định danh và xác thực người dùng sẽ được lưu trữ bằng cách sử dụng mã hóa một chiều (Hash) để ngăn chặn việc giải mã.   - Khi thực hiện mã hóa một chiều, cần thêm và áp dụng một giá trị được tạo ngẫu nhiên gọi là muối cho mật khẩu.  - Giá trị muối không cần bảo mật. Nó sẽ được tạo bằng trình tạo bit ngẫu nhiên và kích thước phải ít nhất là 48 bit.  - Số lần lặp phải được áp dụng càng lớn càng tốt. (ít nhất 1000 lần ) |

Bảo vệ dữ liệu người dùng (FDP)

1. FDP\_IFC.1 Kiểm soát luồng thông tin tập hợp con

|  |  |
| --- | --- |
| Phân cấp | Không có các thành phần khác |
| Các thành phần phụ thuộc | FDP\_IFF.1 Đơn giản hóa các thuộc tính bảo mật |
| FDP\_IFC.1.1 | TSF sẽ thực thi [chính sách kiểm soát luồng thông tin Tường lửa Web] trên [danh sách hoạt động tạo ra luồng thông tin đến/từ chủ thể được kiểm soát được xử lý bởi chủ đề và danh sách thông tin sau đây, và SFP]. a) Chủ thể: Web client b) Thông tin: Lưu lượng web do chủ thể truyền tải c) Hoạt động: Yêu cầu HTTP, HTTPS đến máy chủ web và ứng dụng web |

|  |
| --- |
| Lưu ý áp dụng   * TOE sẽ có thể phát hiện và chặn lưu lượng truy cập bất thường bằng cách xác định xem lưu lượng truy cập web được tạo và truyền bởi người dùng độc hại có bình thường hay không. * TOE phải có khả năng cho phép hoặc chặn lưu lượng truy cập web (HTTP và HTTPS) chảy vào máy chủ web mục tiêu được bảo vệ theo các quy tắc do quản trị viên được ủy quyền đặt. |

1. FDP\_IFF.1 Đơn giản hóa thuộc tính bảo mật

|  |  |
| --- | --- |
| Phân cấp | Không có các thành phần khác |
| Các thành phần phụ thuộc | FDP\_IFC.1 Kiểm soát luồng thông tin tập hợp con  FMT\_MSA.3 Khởi tạo thuộc tính tĩnh |
| FDP\_IFF.1.1 | TSF sẽ thực thi [chính sách kiểm soát luồng thông tin Tường lửa Web] dựa trên các loại chủ đề và thuộc tính bảo mật thông tin sau: [chủ đề sau và danh sách thông tin, chủ đề và các thuộc tính bảo mật thông tin được kiểm soát bởi chính sách kiểm soát luồng thông tin của Tường lửa Web].   1. Chủ thể và thuộc tính bảo mật chủ thể  |  |  | | --- | --- | | Chủ đề | Thuộc tính bảo mật chủ đề | | Máy khách web | {Quyết định bởi Người yêu cầu đánh giá của tuyên bố về các mục tiêu bảo mật} |   b) Thông tin và thuộc tính an toàn thông tin   |  |  | | --- | --- | | Thông tin | Mục tiêu bảo mật thông tin | | Lưu lượng truy cập web được chuyển bởi chủ thể | {Được quyết định bởi Người yêu cầu đánh giá của tuyên bố về các mục tiêu bảo mật} | |
| FDP\_IFF.1.2 | TSF phải cho phép một luồng thông tin giữa chủ thể được kiểm soát và thông tin được kiểm soát thông qua một thao tác được kiểm soát nếu các quy tắc sau được duy trì: [lựa chọn: đối với mỗi thao tác, mối quan hệ dựa trên thuộc tính an toàn phải được duy trì giữa chủ thể và các thuộc tính an toàn thông tin] . |
| FDP\_IFF.1.3 | TSF sẽ thực thi [lựa chọn: các quy tắc SFP kiểm soát luồng thông tin bổ sung]. |
| FDP\_IFF.1.4 | TSF sẽ cấp phép rõ ràng cho luồng thông tin dựa trên các quy tắc sau: [lựa chọn: quy tắc, dựa trên thuộc tính an toàn, cấp phép rõ ràng cho các luồng thông tin]. |
| FDP\_IFF.1.5 | TSF phải từ chối một cách rõ ràng luồng thông tin dựa trên các quy tắc sau: [lựa chọn: các quy tắc, dựa trên các thuộc tính an toàn, từ chối một cách rõ ràng các luồng thông tin]. |

|  |
| --- |
| Lưu ý áp dụng   * TOE sẽ có thể phát hiện và chặn lưu lượng truy cập bất thường bằng cách xác định xem lưu lượng truy cập web được tạo và truyền bởi người dùng độc hại có bình thường hay không.   - TOE sẽ phát hiện và chặn các kiểu tấn công khác nhau, chẳng hạn như danh sách lỗ hổng mới nhất được xuất bản bởi OWASP và các lỗ hổng được xác định bởi các cơ sở đánh giá và tổ chức chứng nhận để yêu cầu các biện pháp bắt buộc.  • Dấu hiệu phát hiện các cuộc tấn công web đã biết và lỗ hổng web sẽ được cung cấp bởi TOE.  - TOE sẽ phát hiện và chặn các cuộc tấn công từ chối dịch vụ HTTP và HTTPS của lớp L7 sau.  • HTTP GET Flooding, CC(Cache-Control) Attack, Slow HTTP Header DoS, Slow HTTP Post DOS, Slow HTTP Read DoS, v.v.  - TOE sẽ phản ứng với các cuộc tấn công dựa trên web để vượt qua các chức năng bảo mật của chính nó như sau.  • Các lỗ hổng IIS Short File/Floder Name Disclosure (tiết lộ thông tin máy chủ web IIS), tấn công Big-HTTP Request, tấn công bằng cách sử dụng các nhận xét SQL đã sửa đổi, kỹ thuật tấn công Method Confusion sử dụng nhầm lẫn giữa phương thức Get và Post, v.v.  - TOE sẽ cung cấp khả năng để cập nhật lên chữ ký mới nhất.   * TOE sẽ có thể cho phép hoặc chặn lưu lượng truy cập web (HTTP và HTTPS) chảy vào máy chủ web mục tiêu được bảo vệ theo các quy tắc do quản trị viên được ủy quyền đặt.   - Quản trị viên có thể đặt quy tắc phát hiện, quy tắc này sẽ hỗ trợ khớp mẫu bằng cách sử dụng biểu thức chính quy.  • Các quy tắc phát hiện và phân tích nội dung cho HTTP 1.0/1.1, HTTP 2.0 và các dịch vụ web (SOAP, WSDL, UDDI, v.v.) sẽ được áp dụng.  - Các luật phát hiện phải có khả năng thiết lập và kiểm soát dựa trên các loại thuộc tính bảo mật cho chủ thể và thông tin.  • Ví dụ về thuộc tính bảo mật chủ đề: *địa chỉ IP, địa chỉ MAC, tên trình duyệt web, phiên bản trình duyệt web, tên hệ điều hành, phiên bản hệ điều hành, v.v.*  • Ví dụ về thuộc tính bảo mật thông tin: *Phương thức, URL, phiên bản HTTP, thông tin tiêu đề yêu cầu (Cookie, Nội dung -Type, v.v.), thông tin nội dung yêu cầu (Message-Body, v.v.)*  - Phương pháp danh sách trắng được khuyến nghị để kiểm soát luồng thông tin của các dịch vụ ứng dụng web (thư mục cụ thể, địa chỉ IP (truyền và nhận)) và phương pháp danh sách đen được khuyến nghị để chặn lưu lượng truy cập web bất thường dựa trên chữ ký.   * TOE sẽ tạo hồ sơ kiểm toán kiểm toán cho các sự kiện kiểm toán chính.   - Hồ sơ kiểm toán về lưu lượng web được phép và bị chặn bởi TOE sẽ được tạo. • Kết quả cho phép và chặn lưu lượng truy cập web bằng FDP\_IFF.1 sẽ được đưa vào. |

1. FDP\_EDI.1 Hành động phản hồi và xác minh tính toàn vẹn của dữ liệu được lưu trữ bên ngoài

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác |
| Các thành phần phụ thuộc | Không có thành phần nào khác |
| FDP\_EDI.1.1 | TSF sẽ xác minh tính toàn vẹn của [lựa chọn : *danh sách dữ liệu người dùng được lưu trữ bên ngoài có thể định cấu hình của quản trị viên* ] |
| FDP\_EDI.1.2 | Khi phát hiện lỗi toàn vẹn dữ liệu người dùng được lưu trữ bên ngoài, TSF sẽ [lựa chọn: *hành động được thực hiện*]. |

|  |
| --- |
| Lưu ý áp dụng   * TOE sẽ xác minh tính toàn vẹn của nội dung web và khi phát hiện lỗi toàn vẹn, nó sẽ thực hiện các hành động phản hồi (*báo động, gửi thư, khôi phục, v.v*.) do quản trị viên được ủy quyền đặt.   - Quản trị viên có thể lựa chọn nội dung trang web cần bảo vệ toàn vẹn (trang chủ, hình ảnh, tệp, v.v.). |

Định danh và xác thực (FIA)

8.1.4.1. FIA\_AFL.1 Xử lý lỗi xác thực

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | FIA\_UAU.1 Định thời gian xác thực FIA\_ |
| AFL.1.1 | TSF sẽ phát hiện khi [lựa chọn: [lựa chọn: số nguyên dương], một số nguyên dương có thể định cấu hình của quản trị viên trong [lựa chọn: phạm vi giá trị được chấp nhận]] xảy ra các nỗ lực xác thực không thành công liên quan đến [lựa chọn: danh sách các sự kiện xác thực]. |
| FIA\_AFL.1.2 | Khi số lần thử xác thực không thành công đã xác định đã được đáp ứng, TSF sẽ [lựa chọn: danh sách các hành động]. |

|  |
| --- |
| Lưu ý áp dụng   * Nếu xác thực người dùng không thành công liên tiếp nhiều lần như số đã đặt trong TOE, các chức năng xác thực và nhận dạng sẽ bị hủy kích hoạt.   - Ví dụ về cách kích hoạt sau khi hủy kích hoạt các chức năng Định danh và xác thực như sau:  • *Kích hoạt trong một khoảng thời gian nhất định sau khi khóa tài khoản*  *• Cung cấp các phương tiện Định danh và xác thực khác để kích hoạt sau khi khóa tài khoản*  - Định danh và xác thực bổ sung phương tiện được lựa chọn trong FIA\_UAU.1 có thể được cung cấp. Trong trường hợp xác thực không thành công với phương tiện Định danh và xác thực bổ sung, nó sẽ được tính vào số lần xác thực người dùng không thành công.  - Số lần xác thực liên tiếp không thành công trong đó Định danh và xác thực bị hủy kích hoạt sẽ được cố định hoặc có thể đặt ở giá trị từ 5 trở xuống.  - Khi thực hiện hủy kích hoạt chức năng xác thực trong một khoảng thời gian nhất định, thời gian cần thiết để kích hoạt lại sẽ được cố định hoặc có thể cài đặt ở giá trị từ 5 phút trở lên.   * Nếu xác thực quản trị viên không thành công liên tiếp nhiều lần như số đã đặt, TOE sẽ thông báo cho quản trị viên thông qua các phương tiện có thể được kiểm tra ngay lập tức.   - Thông báo phải được thực hiện thông qua ít nhất một trong các *báo động, tin nhắn văn bản, e-mail, v.v.* |

8.1.4.2. FIA\_SOS.1 Xác minh bí mật

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| FIA\_SOS.1.1 | TSF sẽ cung cấp cơ chế để xác minh rằng các bí mật đáp ứng [lựa chọn: thước đo chất lượng đã xác định] |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lưu ý áp dụng   * Nếu ID/mật khẩu là phương tiện duy nhất để Định danh và xác thực người dùng, TOE phải đáp ứng các tiêu chí bảo mật của Loại tiêu chí bảo mật mật khẩu(1) khi đăng ký và thay đổi mật khẩu.   <Loại tiêu chí bảo mật mật khẩu(1)>   |  |  |  | | --- | --- | --- | | Mô tả | Nội dung | Ghi chú | | Sự tuân thủ | Bảo mật độ dài hơn 9 chữ số | Bắt buộc | | Chứa ít nhất một số, chữ hoa (tiếng Anh), chữ thường (tiếng Anh) và ký tự đặc biệt | Bắt buộc | | Cấm | Không đặt mật khẩu trùng với tài khoản người dùng (ID) | Bắt buộc | | Cấm nhập lặp lại liên tiếp cùng một chữ cái/số | Bắt buộc | | Cấm nhập tuần tự các chữ cái hoặc số liên tiếp trên bàn phím | Bắt buộc | | Cấm sử dụng lại mật khẩu đã sử dụng ngay trước đó | Thực hiện một trong hai | | Cấm sử dụng lại mật khẩu đã sử dụng trong vòng 3 tháng qua |  * Nếu đầu vào ID/mật khẩu và các chức năng nhận dạng và xác thực bổ sung được thực hiện đồng thời, TOE phải đáp ứng các tiêu chuẩn bảo mật của Loại tiêu chuẩn bảo mật mật khẩu (2) khi đăng ký và thay đổi mật khẩu.   <Loại tiêu chí bảo mật mật khẩu (2)>   |  |  |  | | --- | --- | --- | | Mô tả | Nội dung | Nhận xét | | Sự tuân thủ | Bảo mật độ dài hơn 6 chữ số. | Bắt buộc | | Chứa ít nhất một số, chữ hoa (tiếng Anh), chữ thường (tiếng Anh) và ký tự đặc biệt | Không bắt buộc | | Cấm | Không đặt mật khẩu trùng với tài khoản người dùng (ID) | Bắt buộc | | Cấm nhập lặp lại liên tiếp cùng một chữ cái/số | Không bắt buộc | | Cấm nhập tuần tự các chữ cái hoặc số liên tiếp trên bàn phím | Không bắt buộc | | Cấm sử dụng lại mật khẩu đã sử dụng ngay trước đó | Không bắt buộc | | Cấm sử dụng lại mật khẩu đã sử dụng trong vòng 3 tháng qua | Không bắt buộc | |

8.1.4.3. FIA\_UAU.1 Thời gian xác thực

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | FIA\_UID.1 Thời điểm nhận dạng |
| FIA\_UAU.1.1 | TSF phải cho phép [lựa chọn: danh sách các hành động qua trung gian TSF] thay mặt cho người dùng được thực hiện trước khi người dùng được xác thực. |
| FIA\_UAU.1.2 | TSF sẽ yêu cầu mỗi người dùng phải được xác thực thành công trước khi cho phép bất kỳ hành động nào khác do TSF làm trung gian thay mặt cho người dùng đó, ngoại trừ các hành động được lựa chọn trong FIA\_UAU.1.1. |

|  |
| --- |
| Lưu ý áp dụng   * TOE sẽ cung cấp các chức năng xác thực và nhận dạng dựa trên tài khoản/mật khẩu người dùng để xác minh danh tính của người dùng.   - Việc định danh và xác thực phải được thực hiện để xác nhận rằng người dùng là người dùng hợp pháp của TOE.  - Nếu được yêu cầu xác định và xác thực người dùng tồn tại trong các đại lý hoặc khách hàng cấu thành TOE, giá trị nhận dạng sẽ là một giá trị duy nhất không được đăng ký trùng lặp.  • Khi xác thực người dùng, các thuộc tính bổ sung của đại lý hoặc khách hàng đã đăng ký cũng sẽ được xác thực.  • Các thuộc tính bổ sung: Địa chỉ IP là bắt buộc và ít nhất một trong *các địa chỉ MAC, Số sê-ri và thông tin có thể nhận dạng duy nhất chính tác nhân đó* sẽ được sử dụng bổ sung.   * Trong trường hợp TOE hỗ trợ các phương pháp định danh và xác thực bổ sung, để định danh và xác thực người dùng, TOE phải tự cung cấp các chức năng định danh và xác thực bổ sung hoặc bằng cách tương tác với các thực thể CNTT bên ngoài song song với định danh và xác thực dựa trên tài khoản người dùng và mật khẩu .   - Để cung cấp các chức năng định danh và xác thực bổ sung, có thể sử dụng thiết bị hỗ trợ △2FA tuân thủ các tiêu chuẩn FIDO, △chứng chỉ, △trình tạo mật khẩu dùng một lần (OTP), v.v.  • Nếu nó được hỗ trợ trong môi trường vận hành TOE, nên sử dụng 'thiết bị hỗ trợ 2FA tuân thủ các tiêu chuẩn FIDO'.  - Nếu các chức năng định danh và xác thực bổ sung được cung cấp bởi TOE, thì các chức năng này có thể được cung cấp bằng cách nhận các kết quả xác thực từ bên trong TOE hoặc từ sự tương tác với các thực thể CNTT bên ngoài.  • Nếu TOE cung cấp phương thức sử dụng chứng chỉ, thì việc xác thực chứng chỉ sẽ được thực hiện.  • Thông tin xác thực được sử dụng bởi các thực thể CNTT bên ngoài để thực hiện các phương pháp xác thực và nhận dạng bổ sung sẽ được quản lý an toàn bởi các thực thể CNTT bên ngoài. Nếu TOE lưu trữ thông tin xác thực được sử dụng để thực hiện các phương thức xác thực và nhận dạng bổ sung, các yêu cầu của FPT\_PST.1 sẽ được áp dụng.   * Nếu TOE xác thực các thực thể CNTT bên ngoài, TOE sẽ xác thực các thực thể CNTT bên ngoài tương tác. |

8.1.4.4. FIA\_UAU.4 Cơ chế xác thực sử dụng một lần

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| FIA\_UAU.4.1 | TSF phải ngăn chặn việc sử dụng lại dữ liệu xác thực liên quan đến [lựa chọn: (các) cơ chế xác thực được xác định]. |

|  |
| --- |
| Lưu ý áp dụng   * TOE sẽ ngăn việc sử dụng lại thông tin xác thực của người dùng (*sử dụng dấu thời gian, mã hóa ID phiên, v.v*.)   - Bắt buộc phải áp dụng cho thông tin xác thực được sử dụng để định danh và xác thực dựa trên tài khoản/mật khẩu người dùng được lựa chọn trong FIA\_UAU.1 .  - Nếu TOE nhận thông tin xác thực từ người dùng để cung cấp phương thức xác thực và nhận dạng bổ sung được lựa chọn trong FIA\_UAU.1 thì bắt buộc phải áp dụng cho thông tin xác thực tương ứng.  - Có thể ngăn chặn bằng cách mã hóa ID phiên hoặc đảm bảo tính duy nhất của ID phiên (bao gồm dấu thời gian và giá trị bit ngẫu nhiên, đặt thời gian hết hạn phiên, v.v.)  - Nếu TOE phát hiện nỗ lực sử dụng lại thông tin xác thực bị cấm được sử dụng lại, xác thực sẽ không thành công và một bản ghi kiểm toán sẽ được tạo cho sự kiện lỗi xác thực. |

5.1.4.5. FIA\_UAU.7 Phản hồi xác thực được bảo vệ

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | FIA\_UAU.1 Thời gian xác thực |
| FIA\_UAU.7.1 | TSF sẽ chỉ cung cấp [lựa chọn: danh sách phản hồi] cho người dùng trong khi quá trình xác thực đang diễn ra. |

|  |
| --- |
| Lưu ý áp dụng   * TOE sẽ không hiển thị nội dung khi hiển thị thông tin được sử dụng để xác thực trên thiết bị đầu ra.   - Nó sẽ được áp dụng khi thông tin xác thực được lựa chọn trong FIA\_UAU.1 được hiển thị trên thiết bị đầu ra.  - Thông tin dùng để xác thực được xuất ra dưới dạng *không hiển thị nội dung nhập, hiển thị “\*” thay cho ký tự nhập vào, v.v.*  - Khi người dùng đăng nhập, thông tin xác thực sẽ không bị lộ dưới dạng văn bản thuần túy trong vùng bộ nhớ.   * Trong trường hợp lỗi định danh và xác thực, TOE sẽ không cung cấp phản hồi về nguyên nhân lỗi (*ví dụ: tài khoản (ID) không tồn tại, lỗi mật khẩu, v.v*.). |

8.1.4.6. FIA\_UID.1 Thời gian nhận dạng

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| FIA\_UID.1.1 | TSF phải cho phép [lựa chọn: danh sách các hành động do TSF dàn xếp] thay mặt cho người dùng được thực hiện trước khi người dùng được xác định. |
| FIA\_UID.1.2 | TSF sẽ yêu cầu từng người dùng được xác định thành công trước khi cho phép bất kỳ hành động nào khác do TSF làm trung gian thay mặt cho người dùng đó, ngoại trừ các hành động được lựa chọn trong FIA\_UAU.1.1. |

|  |
| --- |
| Lưu ý áp dụng   * TOE sẽ cung cấp các chức năng xác thực và nhận dạng dựa trên tài khoản/mật khẩu người dùng để xác minh danh tính của người dùng.   - Việc định danh và xác thực phải được thực hiện để xác nhận rằng người dùng là người dùng hợp pháp của TOE.   * Khi hỗ trợ các phương pháp định danh và xác thực bổ sung, TOE sẽ tự cung cấp các chức năng định danh và xác thực bổ sung hoặc kết hợp với các thực thể CNTT bên ngoài, song song với định danh và xác thực dựa trên tài khoản/mật khẩu người dùng. * Nếu TOE xác thực các thực thể CNTT bên ngoài, TOE sẽ xác thực các thực thể CNTT bên ngoài tương tác |

Quản lý bảo mật (FMT)

8.1.5.1. FMT\_MOF.1 Quản lý hành vi chức năng bảo mật

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | FMT\_SMF.1 Đặc tả các chức năng quản lý  FMT\_SMR.1 Các vai trò bảo mật |
| FMT\_MOF.1.1 | TSF phải hạn chế khả năng thực hiện các hành động quản lý của các chức năng [lựa chọn: danh sách các chức năng] cho [quản trị viên được ủy quyền]. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lưu ý áp dụng   * TOE sẽ cung cấp cho người quản trị được ủy quyền các chức năng quản lý an toàn để thiết lập và quản lý các chức năng an toàn, chính sách an toàn, dữ liệu quan trọng, v.v.   - Các chức năng quản lý an toàn bao gồm:  • Chức năng thêm, xóa hoặc thay đổi các điều kiện hoặc các quy tắc có thể xác định hoạt động của chức năng bảo mật.  • Chức năng thêm, xóa hoặc thay đổi các hành động được thực hiện bởi TOE theo các điều kiện hoặc quy tắc.  • Một chức năng để chọn hoặc thay đổi cài đặt TOE  - Các chức năng quản lý bảo mật được thực hiện bởi TOE được hiển thị trong [Bảng 5] bên dưới   |  |  |  | | --- | --- | --- | | Tiểu thể loại | Quản lý an toàn | Ghi chú | | Nhận dạng và xác thực | Đăng ký người dùng, xóa và thay đổi, cấp đặc quyền | Không áp dụng, nếu người dùng đã đăng ký trong TOE là người duy nhất. | | Đặt chính sách độ dài/kết hợp mật khẩu của người dùng | Bắt buộc khi cung cấp chức năng | | Đặt số lần xác thực người dùng không thành công | Bắt buộc khi cung cấp chức năng | | Đặt phương thức phản hồi đối với lỗi xác thực người dùng | Bắt buộc khi cung cấp chức năng | | Đặt thời gian từ khi tắt chức năng xác thực người dùng đến khi kích hoạt lại kích hoạt | Bắt buộc khi cung cấp chức năng | | Thiết lập thông tin xác thực của các thực thể CNTT bên ngoài được xác thực bởi TOE | Bắt buộc khi cung cấp chức năng | | Quản lý bảo mật | Đăng ký IP, xóa và thay đổi thiết bị đầu cuối quản lý |  | | Sao lưu dữ liệu quan trọng, thông tin cấu hình, hồ sơ kiểm tra, v.v. | Bắt buộc khi cung cấp chức năng | | Khôi phục dữ liệu quan trọng, thông tin cấu hình, hồ sơ kiểm tra, v.v. | Bắt buộc khi cung cấp chức năng | | Bật và tắt dịch vụ truy cập quản lý | Bắt buộc khi cung cấp chức năng | | Truy vấn tác nhân - trạng thái, phiên bản và chính sách bảo mật được áp dụng | Bắt buộc khi bao gồm tác nhân | | Quản lý chính sách bảo mật của tác nhân – cài đặt chính sách, truyền chính sách | Bắt buộc khi bao gồm tác nhân | | Cài đặt thông tin xác thực để truy cập vào các thực thể CNTT bên ngoài | Bắt buộc khi cung cấp chức năng | | Tự bảo vệ | Thực hiện tự kiểm tra chức năng bảo mật của TOE theo yêu cầu của quản trị viên | Bắt buộc khi cung cấp chức năng | | Thiết lập hành động phản hồi khi tự kiểm tra thất bại | Bắt buộc khi cung cấp chức năng | | Thực hiện xác minh tính toàn vẹn của các giá trị cài đặt TOE và chính TOE theo yêu cầu của quản trị viên |  | | Thực hiện xác minh tính toàn vẹn của các giá trị cài đặt TOE và chính TOE theo yêu cầu của quản trị viên | Bắt buộc khi cung cấp chức năng | | Cập nhật bảo vệ | Quản trị viên xác thực thủ công các tệp cập nhật | Bắt buộc khi cung cấp chức năng | | Quản trị viên xác thực thủ công các tệp cập nhật | Bắt buộc khi cung cấp chức năng | | Truy vấn thông tin phiên bản TOE |  | | Quản lý phiên an toàn | Cài đặt thời gian khóa phiên người dùng, thời gian chờ phiên người dùng | Bắt buộc khi cung cấp chức năng | | Quản lý phiên an toàn (Trong trường hợp khóa phiên) Xác thực quản trị viên hoặc người dùng cá nhân khi mở khóa phiên |  | | Cài đặt số lượng phiên truy cập đồng thời của người dùng Bắt buộc khi cung cấp chức năng | Bắt buộc khi cung cấp chức năng | | Hồ sơ kiểm toán | Tra cứu hồ sơ kiểm toán |  | | Cài đặt liên quan đến phản hồi đối với việc mất hồ sơ kiểm tra | Bắt buộc khi cung cấp chức năng |   [Bảng 5] Các chức năng quản lý an toàn được triển khai bởi TOE  TOE sẽ cung cấp các chức năng bật/tắt cho tất cả quyền truy cập quản lý.  Nếu bản thân tác nhân có chức năng quản lý bảo mật, máy chủ sẽ có thể bật/tắt chức năng cài đặt tác nhân.  Dịch vụ liên lạc không hỗ trợ các kênh liên lạc được mã hóa sẽ có thể bị vô hiệu hóa. Trong quá trình vận hành TOE, nó sẽ hỗ trợ thực hiện tự kiểm tra định kỳ hoặc theo yêu cầu của người quản trị.  Để đảm bảo hoạt động chính xác, TOE sẽ thực hiện chức năng phản hồi do chính nó thực hiện hoặc chức năng phản hồi do quản trị viên đặt khi quá trình tự kiểm tra không thành công.  TOE sẽ cung cấp cho quản trị viên chức năng thực hiện xác minh tính toàn vẹn  TOE sẽ thực hiện chức năng phản hồi do chính nó thực hiện hoặc chức năng phản hồi do quản trị viên thiết lập khi xác minh tính toàn vẹn không thành công.  Nếu TOE cung cấp chức năng cập nhật trực tuyến hoặc cập nhật thủ công, thì chỉ các tệp cập nhật đã xác thực thành công mới được cài đặt hoặc áp dụng.  Nếu TOE không cung cấp chức năng tự động duy trì phiên bản hiện có khi cài đặt bản cập nhật không thành công, việc phục hồi thủ công bởi quản trị viên sẽ được hỗ trợ.  Các phiên bị khóa sẽ được mở khóa bởi quản trị viên hoặc thông qua chức năng xác thực người dùng cho mỗi phiên, sau khi hết thời gian khóa.  Ngoài ra, TOE có thể cung cấp chức năng gửi bản ghi kiểm tra tới máy chủ nhật ký bên ngoài bởi quản trị viên.  - *Nếu nhật ký hệ thống được hỗ trợ, nó sẽ hỗ trợ truyền mã hóa qua nhật ký hệ thống qua TLS (RFC 5424) hoặc nhật ký hệ thống qua DTLS (RFC 6012).*  - Thuật toán mật mã sử dụng, độ bảo mật khóa mật mã, phương thức lưu trữ khóa mật mã phải đáp ứng yêu cầu ‘Bảo vệ khi lưu trữ khóa mật mã’ của lớp FCS và FPT\_PST.1.  TOE sẽ hạn chế chỉ cho phép các quản trị viên được ủy quyền thực hiện các chức năng quản lý bảo mật có thể thiết lập và quản lý các quy tắc chặn và phát hiện lưu lượng truy cập web.  - Các chức năng quản lý bảo mật như sau.  • Khả năng thêm, xóa hoặc thay đổi các điều kiện hoặc quy tắc hoạt động cho các chức năng bảo mật phát hiện hoặc chặn lưu lượng truy cập web  • Cập nhật chữ ký (mẫu phát hiện)  • Tạo chữ ký mới (mẫu phát hiện)  • Thay đổi ngưỡng tại đó chức năng chặn của TOE vận hành  • Thay đổi thời gian thực hiện hành động chặn lưu lượng • Thay đổi danh sách trắng và danh sách đen địa chỉ hoặc dải IP  • Chức năng thêm, xóa, thay đổi hành động được thực hiện bởi TOE theo điều kiện hoặc quy tắc  - Chức năng xác minh cho đầu vào của quản trị viên các giá trị (hạn chế về ký tự không được chấp nhận, độ dài, v.v.) sẽ được cung cấp. |

8.1.5.2. FMT\_MSA.1 Quản lý thuộc tính bảo mật

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | [FDP\_ACC.1 Kiểm soát truy cập tập hợp con hoặc  FDP\_IFC.1 Kiểm soát luồng thông tin tập hợp con] FMT\_SMF.1 Đặc tả chức năng quản lý  FMT\_SMR.1 Các vai trò bảo mật |
| FMT\_MSA.1.1 | TSF sẽ thực thi [lựa chọn: *kiểm soát truy cập SFP, luồng thông tin kiểm soát SFP*] *để hạn chế khả năng* [lựa chọn: *thay đổi\_mặc định, truy vấn, sửa đổi, xóa,* [lựa chọn: *các thao tác khác*]] các thuộc tính bảo mật [lựa chọn: *danh sách các thuộc tính bảo mật*] cho [Quản trị viên được ủy quyền] |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lưu ý áp dụng   * Người yêu cầu đánh giá sẽ xác định thao tác gán FMT\_MSA.1.1 với tham chiếu đến '[Bảng] Loại quản lý thuộc tính an toàn cho từng thành phần' nếu TOE hỗ trợ các chức năng quản lý thuộc tính an toàn. * Người yêu cầu đánh giá có thể xác định các hành động quản lý thuộc tính bảo mật bổ sung ngoài chức năng quản lý được trình bày trong '[Bảng] Loại quản lý thuộc tính bảo mật cho mỗi thành phần'. Có thể trình bày các hành động quản lý các thuộc tính an toàn cho các yêu cầu bổ sung hoặc mở rộng ngoài các yêu cầu chức năng an toàn được xác định trong tài liệu này.  |  |  |  | | --- | --- | --- | | Các thành phần chức năng bảo mật | Các chức năng quản lý | Các loại quản lý | | FDP\_IFF.1 | Quản lý các thuộc tính được sử dụng để đưa ra quyết định dựa trên quyền truy cập rõ ràng | Quản lý các thuộc tính bảo mật | | FDP\_EDI.1 | Quản lý các thuộc tính dữ liệu được sử dụng cho dữ liệu người dùng được lưu trữ bên ngoài để bảo vệ tính toàn vẹn | Quản lý các thuộc tính bảo mật | | FMT\_MSA.1 | Quản lý các quy tắc theo đó các thuộc tính bảo mật các thuộc tính bảo mật kế thừa các giá trị cụ thể | Quản lý các thuộc tính bảo mật | | FMT\_MSA.3 | Quản lý cài đặt cho phép hoặc hạn chế các giá trị mặc định cho một SFP kiểm soát truy cập nhất định Quản lý các quy tắc theo đó các thuộc tính bảo mật kế thừa các giá trị cụ thể | Quản lý các thuộc tính bảo mật |   < Bảng. Loại quản lý thuộc tính bảo mật cho từng thành phần>   * TOE sẽ có thể cho phép hoặc chặn lưu lượng truy cập web (HTTP và HTTPS) chảy vào máy chủ web mục tiêu được bảo vệ theo các quy tắc do quản trị viên được ủy quyền đặt.   - Quản trị viên có thể đặt quy tắc phát hiện, quy tắc này sẽ hỗ trợ khớp mẫu bằng cách sử dụng biểu thức chính quy.  • Các quy tắc phát hiện và phân tích nội dung cho HTTP 1.0/1.1, HTTP 2.0 và các dịch vụ web (SOAP, WSDL, UDDI, v.v.) sẽ được áp dụng.  - Các luật phát hiện phải có khả năng thiết lập và kiểm soát dựa trên các loại thuộc tính bảo mật cho chủ thể và thông tin.  • Ví dụ về thuộc tính bảo mật chủ đề: địa chỉ IP, địa chỉ MAC, tên trình duyệt web, phiên bản trình duyệt web, tên hệ điều hành, phiên bản hệ điều hành, v.v.  • Ví dụ về thuộc tính bảo mật thông tin: Phương thức, URL, phiên bản HTTP, thông tin tiêu đề được yêu cầu (Cookie, Nội dung -Type, v.v.), thông tin nội dung được yêu cầu (Message-Body, v.v.)  - Phương pháp danh sách trắng được khuyến nghị để kiểm soát luồng thông tin của các dịch vụ ứng dụng web (thư mục cụ thể, địa chỉ IP (truyền và nhận)) và phương pháp danh sách đen được khuyến nghị để chặn lưu lượng truy cập web bất thường dựa trên chữ ký. |

8.1.5.3. FMT\_MSA.3 Khởi tạo thuộc tính tĩnh

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | FMT\_MSA.1 Quản lý các thuộc tính bảo mật  FMT\_SMR.1 Các vai trò bảo mật |
| FMT\_MSA.3.1 | TSF sẽ thực thi [chính sách kiểm soát luồng thông tin tường lửa ứng dụng Web] để cung cấp [lựa chọn, chọn một trong số: hạn chế, cho phép, [lựa chọn: *thuộc tính khác*]] giá trị mặc định cho các thuộc tính bảo mật được sử dụng để thực thi SFP. |
| FMT\_MSA.3.2 | TSF sẽ cho phép [ quản trị viên được ủy quyền ] lựa chọn các giá trị ban đầu thay thế để ghi đè các giá trị mặc định khi một đối tượng hoặc thông tin được tạo. |

|  |
| --- |
| Lưu ý áp dụng  TOE sẽ có thể cho phép hoặc chặn lưu lượng truy cập web (HTTP và HTTPS) chảy vào máy chủ web mục tiêu được bảo vệ theo các quy tắc do quản trị viên được ủy quyền đặt.  - Quản trị viên có thể đặt quy tắc phát hiện, quy tắc này sẽ hỗ trợ khớp mẫu bằng cách sử dụng biểu thức chính quy.  • Các quy tắc phát hiện và phân tích nội dung cho HTTP 1.0/1.1, HTTP 2.0 và các dịch vụ web (SOAP, WSDL, UDDI, v.v.) sẽ được áp dụng.  - Các luật phát hiện phải có khả năng thiết lập và kiểm soát dựa trên các loại thuộc tính bảo mật cho chủ thể và thông tin.  • Ví dụ về thuộc tính bảo mật chủ đề: *địa chỉ IP, địa chỉ MAC, tên trình duyệt web, phiên bản trình duyệt web, tên hệ điều hành, phiên bản hệ điều hành, v.v.*  • Ví dụ về thuộc tính bảo mật thông tin: *Phương thức, URL, phiên bản HTTP, thông tin tiêu đề được yêu cầu (Cookie, Nội dung -Type, v.v.), thông tin nội dung được yêu cầu (Message-Body, v.v.)*  - Phương pháp danh sách trắng được khuyến nghị để kiểm soát luồng thông tin của các dịch vụ ứng dụng web (thư mục cụ thể, địa chỉ IP (truyền và nhận)) và phương pháp danh sách đen được khuyến nghị để chặn lưu lượng truy cập web bất thường dựa trên chữ ký. |

8.1.5.4. FMT\_MTD.1 Quản lý dữ liệu TSF

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | FMT\_SMF.1 Đặc tả chức năng quản lý  FMT\_SMR.1 Các vai trò bảo mật |
| FMT\_MTD.1.1 | TSF phải hạn chế khả năng quản lý [lựa chọn: danh sách dữ liệu TSF] thành [lựa chọn: các vai trò được ủy quyền |

|  |
| --- |
| Lưu ý áp dụng  TOE phải cung cấp cho người quản trị được ủy quyền các chức năng quản lý an toàn để thiết lập và quản lý các chức năng an toàn, chính sách an toàn, dữ liệu quan trọng, v.v.  - Các chức năng quản lý an toàn bao gồm:  • Chức năng thêm, xóa hoặc thay đổi các điều kiện hoặc các quy tắc có thể xác định hoạt động của chức năng bảo mật.  • Chức năng thêm, xóa hoặc thay đổi các hành động được thực hiện bởi TOE theo các điều kiện hoặc quy tắc.  • Một chức năng để chọn hoặc thay đổi các thiết lập TOE  - Các chức năng quản lý an toàn được thực hiện bởi TOE được trình bày trong [Bảng 5]. Người quản trị có thể cấp quyền cho từng người dùng hoặc từng nhóm.  Tài khoản người dùng (ID) là một giá trị duy nhất và sẽ không được đăng ký trùng lặp. Số lần xác thực liên tiếp không thành công trong đó định danh và xác thực bị hủy kích hoạt sẽ được cố định hoặc có thể đặt ở giá trị từ 5 trở xuống.  Khi thực hiện hủy kích hoạt chức năng xác thực trong một khoảng thời gian nhất định, thời gian cần thiết để kích hoạt lại sẽ được cố định hoặc có thể cài đặt ở giá trị từ 5 phút trở lên.  Nếu ID/mật khẩu là phương tiện duy nhất để định danh và xác thực người dùng, TOE phải đáp ứng tiêu chí bảo mật, <Loại tiêu chí bảo mật mật khẩu(1)> của FIA\_SOS.1 khi đăng ký và thay đổi mật khẩu.  Nếu đầu vào ID/mật khẩu và các chức năng định danh và xác thực bổ sung được thực hiện đồng thời, TOE phải đáp ứng tiêu chí bảo mật, <Loại tiêu chí bảo mật mật khẩu(2)> của FIA\_SOS.1 khi đăng ký và thay đổi mật khẩu.  Nếu đầu vào ID/mật khẩu và các chức năng định danh và xác thực bổ sung được thực hiện đồng thời, TOE phải đáp ứng các tiêu chuẩn bảo mật, <Loại tiêu chuẩn bảo mật mật khẩu(2)> của FIA\_SOS.1 khi đăng ký và thay đổi mật khẩu.  Nếu thông tin xác thực cần thiết cho xác thực thực thể CNTT bên ngoài được yêu cầu thiết lập, TOE sẽ cung cấp chức năng thiết lập thông tin cần thiết cho xác thực thực thể CNTT bên ngoài.  - Mục tiêu ứng dụng có thể là khóa chia sẻ trước cho kết nối máy chủ xác thực, mật khẩu xác thực/mã hóa SNMP, v.v.  - Khi mật khẩu được sử dụng để xác thực thực thể CNTT bên ngoài, tiêu chí bảo mật, <Loại Tiêu chí Bảo mật Mật khẩu(1)> hoặc <Loại tiêu chí bảo mật mật khẩu(2)> của FIA\_SOS.1 phải được tuân thủ.  TOE sẽ cung cấp một chức năng để giới hạn IP của các thiết bị đầu cuối quản lý có thể truy cập.  - Địa chỉ IP của các thiết bị đầu cuối quản lý sẽ có thể được đăng ký, xóa hoặc đã thay đổi.  - Các thiết bị đầu cuối quản lý có thể được truy cập bởi quản trị viên chỉ có quyền đọc thay vì cho mục đích quản lý (ví dụ: quản trị viên giám sát, v.v.) có thể được đăng ký và vận hành bổ sung.  - Mỗi lần chỉ có thể thêm một địa chỉ IP máy chủ duy nhất cho các thiết bị đầu cuối quản lý có thể truy cập.  - Phương pháp lựa chọn dải địa chỉ IP, chẳng hạn như 192.168.10.2~253 hoặc đăng ký bằng cách sử dụng 0.0.0.0, 192.168.10.\*, bất kỳ, v.v. có nghĩa là toàn bộ dải mạng không được phép. o Khi cung cấp một chức năng yêu cầu mật khẩu để truy cập các thành phần bên trong của TOE hoặc các thực thể CNTT bên ngoài, TOE sẽ cung cấp chức năng thay đổi mật khẩu mặc định được sử dụng để truy cập các thành phần bên trong hoặc các thực thể CNTT bên ngoài.  - Ví dụ về mật khẩu mặc định bao gồm mật khẩu DBMS và mật khẩu máy chủ web/máy chủ WAS.  - Nếu TOE lưu trữ mật khẩu mặc định để truy cập DBMS, TOE sẽ cung cấp chức năng thay đổi mật khẩu mặc định.  - Ví dụ về thông tin xác thực bao gồm mật khẩu được sử dụng để xác thực TOE trong máy chủ SMTP.  - Tùy thuộc vào việc các chức năng định danh và xác thực bổ sung có được sử dụng đồng thời khi tạo mật khẩu hay không, các tiêu chí bảo mật, <Loại tiêu chí bảo mật mật khẩu(1)> hoặc <Loại tiêu chí bảo mật mật khẩu(2)> của FIA\_SOS.1 sẽ được tuân thủ.  - Nếu một tài khoản (ID) mặc định tồn tại trong TOE để truy cập DBMS/Máy chủ Web/Máy chủ WAS, chức năng thay đổi nó có thể được cung cấp.  Nếu một thực thể CNTT bên ngoài tương tác với TOE yêu cầu thông tin xác thực để xác thực TOE, thì TOE sẽ cung cấp một chức năng để thiết lập thông tin xác thực cần thiết để được xác thực bởi thực thể CNTT bên ngoài.  - Ví dụ về thông tin xác thực bao gồm mật khẩu được sử dụng để xác thực TOE trong máy chủ SMTP.  - Mật khẩu nên tuân thủ các tiêu chí bảo mật, <Loại tiêu chí bảo mật mật khẩu (2)> của FIA\_SOS.1.  • Tuy nhiên, ngay cả các ký tự có trong tiêu chí bảo mật mật khẩu cũng không được bao gồm các ký tự không được phép nhập bởi thực thể CNTT bên ngoài tương tác.  TOE sẽ cung cấp giao diện chỉ cho phép quản trị viên được ủy quyền truy cập cài đặt TOE và những người khác không phải quản trị viên được ủy quyền sẽ không thể truy cập cài đặt TOE.  - Access có nghĩa là các thao tác như đọc, thay đổi và xóa, v.v.  Khi cung cấp chức năng sao lưu các cài đặt TOE ở dạng tệp bên ngoài, một chức năng mã hóa sẽ được cung cấp.  Đối với mã hóa, thuật toán mã hóa được sử dụng, bảo mật khóa mã hóa và phương thức lưu trữ khóa mã hóa phải đáp ứng yêu cầu 'bảo vệ khi lưu trữ khóa mã hóa' của lớp FCS và FPT\_PST.1.  TOE sẽ cung cấp một chức năng để người quản trị kiểm tra nội dung và kết quả của việc xác minh tính toàn vẹn.  - Nội dung và kết quả xác minh tính toàn vẹn được xác nhận thông qua màn hình hiển thị, hồ sơ kiểm toán.  TOE sẽ cung cấp chức năng để người dùng kiểm tra 'thông tin nhận dạng duy nhất của TOE'.  - Thông tin nhận dạng TOE phải là duy nhất, người dùng có thể kiểm tra thông qua giao diện và không thể sửa đổi, thay đổi. Nó sẽ bao gồm những điều sau:  • Tên TOE, phiên bản TOE, bản phát hành TOE hoặc số bản dựng  - Nếu TOE bao gồm nhiều thành phần được tách biệt về mặt vật lý, thông tin nhận dạng của mỗi thành phần phải là duy nhất, có thể được kiểm tra và không thể sửa đổi hoặc thay đổi bởi người dùng. Nó sẽ bao gồm những điều sau:  • Tên và phiên bản của TOE bao gồm thành phần, tên thành phần, phiên bản thành phần và số bản phát hành hoặc bản dựng của thành phần  - Một hệ thống quản lý phiên bản sẽ được áp dụng để kiểm tra bản vá của TOE/các thành phần và liệu các chức năng có được cải thiện hay không. (ví dụ: Trong trường hợp cải tiến chức năng và bản vá, một hệ thống thay đổi phiên bản chính, phiên bản phụ, số phát hành và số bản dựng cho từng trường hợp được thiết lập để theo dõi lý do thay đổi TOE/thành phần với thông tin phiên bản)  - Trong trường hợp thiết bị phần cứng, người dùng sẽ có thể xem thông tin nhận dạng duy nhất của phần sụn ngoài thông tin nhận dạng TOE thông qua giao diện TOE.  Một lượng thời gian nhất định, là lượng thời gian tích lũy sau khi kết nối kích hoạt khóa phiên người dùng hoặc hết thời gian phiên, quản trị viên có thể sửa lượng thời gian tích lũy từ giá trị 10 phút trở xuống hoặc đặt theo tỷ lệ đến số lần xác thực thất bại.  Hồ sơ kiểm tra chỉ được truy vấn thông qua chức năng an toàn do TOE cung cấp.  Các lệnh giao diện người dùng (UI) và CLI có liên quan sẽ không được cung cấp để ngay cả quản trị viên được ủy quyền cũng không thể xóa hoặc thay đổi hồ sơ kiểm tra.  Ví dụ về các điều kiện để thông báo cho quản trị viên liên quan đến phản hồi mất hồ sơ kiểm toán như sau.  - 90% trở lên của dung lượng đĩa thiết lập, 100 MB trở lên, v.v.  TOE sẽ hạn chế chỉ cho phép quản trị viên được ủy quyền thực hiện các chức năng quản lý bảo mật có thể thiết lập và quản lý các quy tắc chặn và phát hiện lưu lượng truy cập web.  - Các chức năng quản lý bảo mật như sau.  • Khả năng thêm, xóa hoặc thay đổi các điều kiện hoặc quy tắc hoạt động cho các chức năng bảo mật phát hiện hoặc chặn lưu lượng truy cập web  • Cập nhật chữ ký (mẫu phát hiện)  • Tạo chữ ký mới (mẫu phát hiện)  • Thay đổi ngưỡng tại đó chức năng chặn của TOE vận hành  • Thay đổi thời gian thực hiện hành động chặn lưu lượng  • Thay đổi danh sách trắng và danh sách đen địa chỉ hoặc dải IP  • Chức năng thêm, xóa, thay đổi hành động được thực hiện bởi TOE theo điều kiện hoặc quy tắc  - Chức năng xác minh cho đầu vào của quản trị viên các giá trị (hạn chế về ký tự không được chấp nhận, độ dài, v.v.) sẽ được cung cấp |

8.1.5.5. FMT\_PWD.1 Quản lý ID và mật khẩu (Mở rộng)

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | FMT\_SMF.1 Đặc tả chức năng quản lý  FMT\_SMR.1 Vai trò bảo mật |
| FMT\_PWD.1.1 | TSF phải hạn chế khả năng quản lý mật khẩu của [lựa chọn: *danh sách các chức năng*] đối với [quản trị viên được ủy quyền].  1. [lựa chọn: *quy tắc kết hợp mật khẩu và/hoặc độ dài*]  2. [lựa chọn: *quản lý khác như quản lý các ký tự đặc biệt không sử dụng được cho mật khẩu, v.v*.] |
| FMT\_PWD.1.2 | TSF sẽ hạn chế khả năng quản lý ID của [lựa chọn: *danh sách các chức năng*] cho [quản trị viên được ủy quyền].  1. [lựa chọn: *quy tắc kết hợp ID và/hoặc độ dài*]  2. [lựa chọn: *quản lý khác như quản lý các ký tự đặc biệt không sử dụng được cho ID, v.v*.] |
| FMT\_PWD.1.3 | TSF sẽ cung cấp khả năng cho [lựa chọn*: thiết lập ID và mật khẩu khi cài đặt, đặt mật khẩu khi cài đặt, đổi ID và mật khẩu khi người được cấp quyền truy cập lần đầu, đổi mật khẩu khi người được cấp quyền truy cập lần đầu*]. |

|  |
| --- |
| Lưu ý áp dụng  Tài khoản người dùng (ID) là một giá trị duy nhất và sẽ không được đăng ký trùng lặp.  TOE sẽ cung cấp chức năng buộc thay đổi/tạo mật khẩu mặc định của quản trị viên trong lần truy cập ban đầu (truy cập quản lý, truy cập cục bộ) tới TOE.  - Nếu có mật khẩu mặc định, chức năng thay đổi mật khẩu mặc định sẽ được cung cấp trong lần truy cập ban đầu vào TOE, sau đó sẽ có thể quản lý và truy cập cục bộ vào TOE.  - Nếu không có mật khẩu mặc định, mật khẩu mới sẽ được tạo, sau đó có thể quản lý và truy cập cục bộ vào TOE.  • Mật khẩu phải tuân thủ các tiêu chí bảo mật, <Loại Tiêu chí Bảo mật Mật khẩu (1)> hoặc <Loại Tiêu chí Bảo mật Mật khẩu (2)> của FIA\_SOS.1.  - Nếu không có tài khoản (ID) mặc định, một tài khoản (ID) mới sẽ được tạo, sau đó có thể quản lý và truy cập cục bộ vào TOE |

8.1.5.6. FMT\_SMF.1 Đặc tả chức năng quản lý

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác |
| Phụ thuộc | Không phụ thuộc. |
| FMT\_SMF.1.1 | TSF phải có khả năng thực hiện các chức năng quản lý sau: [lựa chọn: *danh sách các chức năng quản lý được cung cấp bởi TSF*] |

5.1.5.7. FMT\_SMR.1 Vai trò bảo mật

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | FIA\_UID.1 Định thời gian nhận dạng |
| FMT\_SMR.1.1 | TSF sẽ duy trì các vai trò [lựa chọn: các vai trò được xác định có thẩm quyền]. |
| FMT\_SMR.1.2 | TSF sẽ có thể liên kết người dùng và vai trò của họ được xác định trong FMT\_SMR.1.1. |

Bảo vệ TSF (FPT)

8.1.6.1. FPT\_PST.1 Bảo vệ cơ bản dữ liệu TSF được lưu trữ (Mở rộng)

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Phụ thuộc | Không có phụ thuộc. |
| FPT\_PST.1.1 | TSF phải bảo vệ [lựa chọn: *dữ liệu TSF*] được lưu trữ trong các thùng chứa do TSF kiểm soát khỏi việc *tiết lộ, sửa đổi trái phép* |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lưu ý áp dụng  1. Bảo vệ khi lưu trữ dữ liệu TSF (thông tin quan trọng)  TOE sẽ lưu trữ thông tin quan trọng theo cách an toàn khi lưu trữ bên trong TOE.  - Ít nhất khi TOE lưu trữ các thông tin quan trọng sau đây, nó sẽ được mã hóa và lưu trữ. • Mật khẩu được TOE sử dụng để định danh và xác thực người dùng  • Thông tin xác thực được TOE sử dụng để định danh và xác thực bổ sung  • Khóa mã hóa dữ liệu (DEK)  - Khóa mã hóa dữ liệu (DEK) sẽ được mã hóa và lưu trữ bằng khóa mã hóa chính (KEK)  - Các yêu cầu liên quan đến việc tạo và lưu trữ khóa mã hóa khóa (KEK) phải đáp ứng yêu cầu 'bảo vệ khi lưu trữ khóa mã hóa' của FCS\_CKM.1(1), FCS\_CKM.1(2) và FPT\_PST.1.  - Khi TOE lưu trữ các thông tin sau, nó phải được lưu trữ bằng cách sử dụng mã hóa, kiểm soát truy cập, v.v.  • Thông tin được sử dụng để xác thực lẫn nhau khi TOE và các thực thể CNTT bên ngoài tương tác  • Cần có mật khẩu quản trị viên của máy chủ DBMS/máy chủ web/máy chủ WAS cho TOE để truy cập DBMS/máy chủ web/máy chủ WAS tồn tại bên trong hoặc bên ngoài TOE.  • Khóa mã hóa (khóa chia sẻ trước, khóa đối xứng, khóa riêng)  - Mật khẩu người dùng được TOE sử dụng để định danh và xác thực người dùng sẽ được lưu trữ bằng cách sử dụng mã hóa một chiều (băm) để ngăn chặn việc giải mã.  • Khi thực hiện mã hóa một chiều, cần thêm và áp dụng một giá trị được tạo ngẫu nhiên gọi là muối vào mật khẩu.  • Giá trị muối không cần bảo mật. Nó sẽ được tạo bằng cách sử dụng bộ tạo bit ngẫu nhiên và kích thước phải ít nhất là 48 bit.  • Số lần lặp phải được áp dụng càng lớn càng tốt (ít nhất 1000 lần).  - Mật khẩu quản trị viên của máy chủ DBMS/máy chủ Web/máy chủ WAS, v.v. cần thiết cho hoạt động của TOE có thể được lưu trữ sau khi được mã hóa bằng cách áp dụng thuật toán mã hóa khóa công khai/khóa đối xứng.  - Khóa mã hóa có nghĩa là khóa chia sẻ trước, khóa đối xứng, khóa riêng, v.v. và bao gồm tất cả các khóa được sử dụng để truy cập quản lý TOE/truy cập cục bộ và cài đặt tương tác giữa các thành phần TOE.  - Mật khẩu và khóa mã hóa có trong thông tin quan trọng tối thiểu sẽ được mã hóa sẽ không được lưu trữ trong TOE bằng cách mã hóa cứng.  - Thuật toán mật mã sử dụng, độ bảo mật khóa mật mã và phương thức lưu trữ khóa mật mã phải đáp ứng yêu cầu “bảo vệ khi lưu trữ khóa mật mã” của lớp FCS và FPT\_PST.1.  2. Bảo vệ khi lưu trữ dữ liệu TSF (cài đặt, bản ghi kiểm toán)  TOE sẽ cung cấp chức năng để bảo vệ các giá trị cài đặt TOE được lưu trữ (chính sách bảo mật, tham số cài đặt môi trường, v.v.) để chỉ quản trị viên được ủy quyền mới có thể truy cập.  - Đối với TOE kiểu thiết bị phần cứng, cài đặt TOE được lưu trữ bên trong sẽ được bảo vệ và đối với TOE kiểu phần mềm, cài đặt TOE được lưu trữ trong cửa hàng do TOE kiểm soát sau khi cài đặt.  - TOE sẽ cung cấp giao diện chỉ cho phép quản trị viên được ủy quyền truy cập cài đặt TOE và những người khác không phải quản trị viên được ủy quyền sẽ không thể truy cập cài đặt TOE  • Truy cập có nghĩa là các thao tác như đọc, thay đổi, xóa, v.v.  - Khi cung cấp chức năng để sao lưu cài đặt TOE ở dạng tệp bên ngoài, chức năng mã hóa sẽ được cung cấp.  - Trong quá trình mã hóa, thuật toán mã hóa được sử dụng, độ an toàn của khóa mã hóa và phương thức lưu trữ khóa mã hóa phải đáp ứng yêu cầu 'bảo vệ khi lưu trữ khóa mã hóa' của lớp FCS và FPT\_PST.1.  Nếu WAS (Tomcat, Jesus, v.v.) được bao gồm trong gói TOE, TOE sẽ thực hiện không bao gồm thông tin quan trọng trong nhật ký WAS.  - Thông tin quan trọng như mật khẩu và khóa mã hóa không được để ở dạng văn bản thuần túy trong nhật ký WAS.  TOE có thể mã hóa và lưu trữ hồ sơ kiểm tra một cách an toàn khi chúng được lưu trữ bên trong TOE.  - Thuật toán mật mã sử dụng, độ bảo mật khóa mật mã và phương thức lưu trữ khóa mật mã phải đáp ứng yêu cầu “bảo vệ khi lưu trữ khóa mật mã” của lớp FCS và FPT\_PST.1. 3. Bảo vệ khi lưu trữ khóa mật mã  TOE sẽ lưu trữ khóa mật mã một cách an toàn.  - Khóa mã hóa dữ liệu (DEK) có thể được lưu trữ bằng cách sử dụng khóa mã hóa khóa (KEK).  - Khóa mã hóa khóa (KEK) có thể được tạo qua nhiều giai đoạn của chuỗi khóa, trong đó khóa mã hóa khóa cuối cùng (KEK) có thể được mã hóa và lưu trữ bằng khóa mã hóa khóa (KEK) của giai đoạn trước.  - Không thể lưu trữ khóa mã hóa khóa (KEK) ngoại trừ khóa mã hóa khóa cuối cùng (KEK) trong chuỗi khóa.  - Khi khóa mật mã được lưu trữ bên ngoài TOE, nên sử dụng phương tiện lưu trữ đã được xác minh về độ an toàn như thẻ thông minh, USB bảo mật và mã thông báo bảo mật (HSM).  • Nên sử dụng sản phẩm đã nhận được báo cáo kiểm tra chức năng bảo mật hoặc chứng chỉ CC trong nước/nước ngoài cho phương tiện lưu trữ.  - Mã hóa cứng và lưu trữ khóa mã hóa trong TOE là không được phép.  - Như thể hiện trong [Bảng 6] bên dưới, người đăng ký phải xác định tất cả các khóa mật mã được sử dụng để lưu trữ và truyền trong TOE, đồng thời chứng minh tính bảo mật bằng cách gửi danh sách và tài liệu giải thích về các phương pháp lưu trữ và hủy khóa.   |  |  | | --- | --- | | Loại khóa mật mã | Cách lưu trữ và hủy khóa | | Khóa riêng TLS | - Loại: Khóa riêng RSA  - Trình tạo: Được tạo bởi TOE  - Lưu trữ/Bảo vệ: Lưu trữ trong TOE/Chặn truy cập trái phép vào khu vực lưu trữ TOE  - Hủy: Ghi đè 3 lần bằng 0 và 1 khi thực hiện lệnh hủy khóa | | Khóa mã hóa phiên TLS | - Loại: Khóa ARIA  - Trình tạo: Được tạo bởi TOE  - Lưu trữ/Bảo vệ: Chỉ lưu trữ trong bộ nhớ (RAM)  - Hủy: Ghi đè 3 lần bằng 0 và 1 khi kết thúc phiên | | Khóa xác minh tính toàn vẹn của phiên TLS | - Loại: Khóa HMAC  - Trình tạo: Được tạo bởi TOE  - Lưu trữ/Bảo vệ: Chỉ lưu trữ trong bộ nhớ (RAM)  - Hủy: Ghi đè 3 lần bằng 0 và 1 khi kết thúc phiên |   [Bảng 6] Cách lưu trữ và hủy khóa mật mã  - Khi TOE lưu trữ các khóa mật mã (khóa chia sẻ trước, khóa đối xứng, khóa riêng, v.v.) được sử dụng để truy cập cục bộ/quản trị để quản lý TOE và để cài đặt tương tác với thiết bị riêng biệt, nó sẽ được bảo vệ và lưu trữ theo cách như *mã hóa, kiểm soát truy cập, v.v.* |

8.1.6.2. FPT\_RCV.2 Phục hồi tự động

|  |  |
| --- | --- |
| Phân cấp cho | FRP\_RCV.1 Khôi phục thủ công |
| Phần phụ thuộc | AGD\_OPE.1 Hướng dẫn người dùng vận hành |
| FPT\_RCV.2.1 | Khi không thể khôi phục tự động từ [lựa chọn: danh sách lỗi/gián đoạn dịch vụ], TSF sẽ chuyển sang chế độ bảo trì trong đó khả năng quay lại trạng thái an toàn trạng thái được cung cấp. |
| FPT\_RCV.2.2 | Đối với [lựa chọn: danh sách lỗi/gián đoạn dịch vụ], TSF phải đảm bảo đưa TOE trở lại trạng thái an toàn bằng cách sử dụng các thủ tục tự động |

|  |
| --- |
| Lưu ý áp dụng  TOE sẽ cung cấp chức năng để cập nhật chữ ký mới nhất.  Nếu chức năng cập nhật được cung cấp, TOE sẽ cung cấp chức năng tự động duy trì phiên bản hiện có khi cài đặt cập nhật không thành công.  - Nếu nó không được hỗ trợ bởi TOE, việc khôi phục thủ công bởi quản trị viên sẽ được hỗ trợ.  - Nhà tài trợ sẽ mô tả chi tiết quy trình khôi phục thủ công của quản trị viên trong các sản phẩm bàn giao |

8.1.6.3. FPT\_TST.1 Kiểm tra TSF

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Phụ thuộc | Không có phụ thuộc. |
| FPT\_TST.1.1 | TSF sẽ chạy một bộ tự kiểm tra [lựa chọn: *ở lần khởi động ban đầu, định kỳ trong quá trình hoạt động bình thường, theo yêu cầu của người dùng được ủy quyền, ở các điều kiện [lựa chọn: điều kiện theo đó việc tự kiểm tra sẽ xảy ra*] để chứng minh hoạt động chính xác của [lựa chọn: [lựa chọn: *các bộ phận của TSF], TSF*]. |
| FPT\_TST.1.2 | TSF sẽ cung cấp cho người dùng được ủy quyền khả năng xác minh tính toàn vẹn của [lựa chọn: [lựa chọn: *các phần của dữ liệu TSF], dữ liệu TSF*]. |
| FPT\_TST.1.3 | TSF sẽ cung cấp cho người dùng được ủy quyền khả năng xác minh tính toàn vẹn của [lựa chọn: [lựa chọn: *các phần của TSF], TSF*] |

|  |
| --- |
| Lưu ý áp dụng  1. Tự kiểm tra máy chủ TOE, chức năng phản hồi và tạo bản ghi kiểm tra  TOE sẽ thực hiện tự kiểm tra trong quá trình khởi động (hoặc thực thi)/vận hành ban đầu theo định kỳ hoặc theo yêu cầu của quản trị viên.  - Khi khởi động (hoặc thực thi) TOE lần đầu bắt buộc phải thực hiện tự kiểm tra và trong quá trình vận hành phải hỗ trợ thực hiện tự kiểm tra định kỳ hoặc theo yêu cầu của người quản trị.  - Mục tiêu tự kiểm tra có nghĩa là quy trình chính của TOE và phải kiểm tra xem quy trình có chạy bình thường không.  - Đối tượng tự kiểm tra có thể được lựa chọn bởi người nộp đơn, nhưng nếu trạng thái bất thường của thực thể (ví dụ: lỗi, dừng, v.v.) ảnh hưởng đến chức năng bảo mật của TOE, thì thực thể tương ứng sẽ được đưa vào làm đối tượng tự kiểm tra Bài kiểm tra.  - Lịch sử tự kiểm tra sẽ được xác nhận thông qua đầu ra màn hình, hồ sơ kiểm tra.  - TOE kiểu thiết bị phần cứng phải đáp ứng các yêu cầu sau.  • Tự kiểm tra sẽ được thực hiện để phát hiện lỗi trong phần cứng (ví dụ: bộ nhớ, flash, NIC, v.v.) và phần mềm (ví dụ: quy trình, v.v.) được bao gồm trong phạm vi của TOE khi khởi động và trong khi vận hành TOE.  - Nếu tồn tại các thành phần TOE tách biệt về mặt vật lý, việc tự kiểm tra sẽ được thực hiện bằng cách chọn các đối tượng bao gồm tất cả các thành phần.  - Nhà tài trợ mô tả chi tiết chức năng tự kiểm tra trong hồ sơ đệ trình.  Nếu kết quả tự kiểm tra TOE không thành công, nó sẽ thực hiện chức năng phản hồi.  - TOE sẽ thực hiện chức năng phản hồi đã triển khai hoặc chức năng phản hồi do quản trị viên thiết lập để đảm bảo hoạt động chính xác.  - Hồ sơ kiểm tra sẽ được tạo ra cho kết quả tự kiểm tra.  - Ví dụ về các chức năng phản hồi được thực hiện khi kết quả tự kiểm tra là lỗi như sau. • Chấm dứt chương trình, hiển thị màn hình thông báo cảnh báo, khởi động lại quá trình, v.v.  - Chức năng quản lý bảo mật có thể được cung cấp để quản trị viên thiết lập chức năng phản hồi.  2. Xác minh tính toàn vẹn của máy chủ TOE, chức năng phản hồi và tạo bản ghi kiểm tra  TOE sẽ cung cấp chức năng để xác minh tính toàn vẹn của chính nó và các giá trị cài đặt của nó.  - Xác minh tính toàn vẹn bao gồm các giá trị cài đặt TOE (tệp cấu hình, v.v.) và bản thân TOE (quy trình, thư viện, tệp thực thi, v.v.).  - Xác minh tính toàn vẹn sẽ được thực hiện khi TOE được thực thi lần đầu (hoặc khởi động) và xác minh tính toàn vẹn định kỳ có thể được thực hiện bổ sung.  - Đối tượng xác minh tính toàn vẹn có thể được nhà tài trợ lựa chọn, nhưng nếu trạng thái bất thường của thực thể (ví dụ: lỗi, dừng, v.v.) ảnh hưởng đến chức năng an toàn của TOE, thì thực thể tương ứng sẽ được đưa vào làm đối tượng xác minh tính toàn vẹn.  - Nếu tồn tại các thành phần TOE tách biệt về mặt vật lý, việc xác minh tính toàn vẹn sẽ được thực hiện bằng cách chọn các đối tượng để bao gồm tất cả các thành phần.  - Phải cung cấp chức năng để người quản trị thực hiện xác minh tính toàn vẹn.  - Thuật toán mật mã được sử dụng, độ an toàn của khóa mật mã và phương thức lưu trữ khóa mật mã phải đáp ứng các yêu cầu về “bảo vệ khi lưu trữ khóa mật mã” của lớp FCS và FPT\_PST.1.  Nếu nhân hệ điều hành hoặc mô-đun mức nhân được bao gồm trong phạm vi của TOE, thì TOE sẽ cung cấp chức năng để xác minh tính toàn vẹn của nhân hệ điều hành hoặc mô-đun mức nhân.  - Khi xác minh tính toàn vẹn bằng phương pháp so sánh giá trị băm, thuật toán mật mã được sử dụng, bảo mật khóa mật mã và phương thức lưu trữ khóa mật mã phải đáp ứng các yêu cầu về “bảo vệ khi lưu trữ khóa mật mã” của lớp FCS và FPT\_PST.1.  TOE sẽ cung cấp chức năng cho quản trị viên để kiểm tra nội dung và kết quả của việc xác minh tính toàn vẹn.  - Nội dung và kết quả xác minh tính toàn vẹn sẽ được kiểm tra thông qua màn hình hiển thị và hồ sơ kiểm toán.  TOE sẽ thực hiện chức năng phản hồi nếu xác minh tính toàn vẹn không thành công.  - TOE sẽ thực hiện chức năng phản hồi được triển khai của chính nó hoặc chức năng phản hồi do quản trị viên thiết lập.  - Hồ sơ kiểm tra sẽ được tạo ra cho kết quả xác minh tính toàn vẹn.  - Ví dụ về các chức năng phản hồi được thực hiện khi kết quả xác minh tính toàn vẹn bị lỗi như sau.  • Ngắt chương trình thực thi, hiển thị màn hình thông báo cảnh báo, v.v.  - Chức năng quản lý bảo mật có thể được cung cấp để quản trị viên thiết lập chức năng phản hồi |

8.1.6.4. Cập nhật bản vá bảo mật FPT\_TUD.1 TSF (Mở rộng)

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Phụ thuộc | Không có phụ thuộc. |
| FPT\_TUD.1.1 | TSF sẽ cung cấp [lựa chọn: vai trò được ủy quyền] với chức năng hỏi thông tin nhận dạng duy nhất của TOE. |
| FPT\_TUD.1.2 | TSF sẽ xác minh tính hợp lệ của các tệp cập nhật bằng cách sử dụng [lựa chọn: *so sánh giá trị băm, xác minh chữ ký số, [lựa chọn: cơ chế xác thực an toàn khác]* ] trước khi cài đặt các bản cập nhật |

|  |
| --- |
| Lưu ý áp dụng  TOE sẽ cung cấp một chức năng cho người dùng để kiểm tra ‘thông tin nhận dạng duy nhất của TOE’.  - Thông tin nhận dạng TOE phải là duy nhất, người dùng có thể kiểm tra thông qua giao diện và không thể chỉnh sửa hoặc thay đổi. Nó sẽ bao gồm những điều sau đây.  • Tên TOE, phiên bản TOE, số bản phát hành hoặc bản dựng TOE  - Nếu TOE bao gồm nhiều thành phần được tách biệt về mặt vật lý, thông tin nhận dạng của từng thành phần phải là duy nhất, có thể được kiểm tra và người dùng không thể sửa đổi hoặc thay đổi. Nó sẽ bao gồm những điều sau:  • Tên và phiên bản của TOE bao gồm thành phần, Tên thành phần, Phiên bản thành phần, Số bản phát hành hoặc bản dựng thành phần.  - Nên áp dụng một hệ thống quản lý phiên bản có thể kiểm tra xem TOE và các thành phần TOE có được vá lỗi và cải tiến chức năng hay không.  (ví dụ: Trong trường hợp cải thiện bản vá và chức năng, hệ thống thay đổi phiên bản chính phiên bản phụ, số phát hành và số bản dựng cho từng trường hợp được thiết lập để theo dõi lý do thay đổi các thành phần TOE/TOE với thông tin phiên bản)  - Trong trường hợp thiết bị phần cứng, người dùng sẽ có thể xem thông tin nhận dạng duy nhất của phần sụn ngoài thông tin nhận dạng TOE thông qua giao diện TOE.  TOE sẽ cung cấp chức năng cập nhật chữ ký mới nhất.  Trong trường hợp cung cấp chức năng cập nhật, TOE sẽ xác minh tính hợp lệ của các tệp cập nhật TOE trước khi cài đặt hoặc áp dụng các tệp cập nhật.  - Nếu TOE cung cấp chức năng cập nhật trực tuyến hoặc cập nhật thủ công, thì chỉ các tệp cập nhật đã thành công trong việc xác minh tính hợp lệ mới được cài đặt hoặc áp dụng.  - Xác minh tính toàn vẹn là bắt buộc khi xác minh tính hợp lệ của các tệp cập nhật và sẽ được thực hiện bằng xác minh chữ ký số, xác minh giá trị băm công khai, v.v.  - Khi xác minh chữ ký số, xác minh tính hợp lệ của chứng chỉ (trong vòng 1 năm hiệu lực ) Sẽ được thực hiện.  - Thuật toán mật mã và bảo mật khóa mật mã phải đáp ứng các yêu cầu của lớp FCS. - Kết quả xác nhận hồ sơ cập nhật (thành côngthất bại) sẽ được kiểm toán và ghi lại.  Nếu chức năng cập nhật được cung cấp, TOE sẽ cung cấp chức năng tự động duy trì phiên bản hiện có khi cài đặt cập nhật không thành công.  - Một bản ghi kiểm tra sẽ được tạo cho kết quả cài đặt bản cập nhật và lý do thất bại.  - Nếu nó không được hỗ trợ bởi TOE, việc khôi phục thủ công bởi quản trị viên sẽ được hỗ trợ.  - Nhà phát triển sẽ mô tả chi tiết quy trình khôi phục thủ công của quản trị viên trong các sản phẩm bàn giao. |

Truy cập TOE (FTA)

8.1.7.1. FTA\_MCS.2 Giới hạn thuộc tính cho mỗi người dùng trên nhiều phiên đồng thời

|  |  |
| --- | --- |
| Phân cấp cho | FTA\_MCS.1 Giới hạn cơ bản đối với nhiều phiên đồng thời |
| Phụ thuộc | FIA\_UID.1 Thời gian nhận dạng |
| FTA\_MCS.2.1 | TSF sẽ hạn chế số phiên đồng thời tối đa thuộc về cùng một người dùng theo các quy tắc [giới hạn số phiên đồng thời tối đa là 1 đối với những người dùng có cùng đặc quyền và cùng một người dùng, quy định về số phiên đồng thời tối đa {do Người yêu cầu đánh giá xác định}]. |
| FTA\_MCS.2.2 | TSF sẽ thực thi giới hạn [1] phiên cho mỗi người dùng theo mặc định |

|  |
| --- |
| Lưu ý áp dụng  TOE sẽ không cho phép truy cập trùng lặp vào TOE với cùng một tài khoản người dùng hoặc cùng một đặc quyền.  - Nếu người dùng đăng nhập bằng cùng một tài khoản trên một thiết bị đầu cuối khác sau khi đăng nhập, phải chặn truy cập mới hoặc chấm dứt truy cập trước đó.  - Đăng nhập trùng lặp với cùng một đặc quyền sẽ không được phép.  - Một bản ghi kiểm toán sẽ được tạo khi truy cập trùng lặp bị chặn |

5.1.7.2. FTA\_TSE.1(1) Thiết lập phiên TOE

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Phụ thuộc | Không có phụ thuộc. |
| FTA\_TSE.1.1 | TSF sẽ có thể từ chối **thiết lập phiên truy cập quản lý của quản trị viên** dựa trên [IP truy cập, [lựa chọn: [lựa chọn: *thuộc tính chức năng quản lý quan trọng], không*]] |

|  |
| --- |
| Lưu ý áp dụng  TOE sẽ cung cấp chức năng hạn chế IP của các thiết bị đầu cuối quản lý có thể truy cập.  - Có thể đăng ký, xóa, thay đổi địa chỉ IP của các thiết bị đầu cuối quản lý.  - Các thiết bị đầu cuối quản lý có thể truy cập được đối với quản trị viên chỉ có quyền truy cập đọc thay vì cho mục đích quản lý (ví dụ: *quản trị viên giám sát*) có thể được đăng ký bổ sung để hoạt động.  - IP của các thiết bị đầu cuối quản lý có thể truy cập có thể được thêm từng cái một dưới dạng IP máy chủ.  - Không được phép đăng ký bằng cách lựa chọn dải địa chỉ IP như 192.168.10.2~253 hoặc bằng cách sử dụng 0.0.0.0, 192.168.10.\*, bất kỳ, nghĩa là toàn bộ dải mạng. |

Các yêu cầu chức năng an toàn (SFR bắt buộc có điều kiện)

'SFR bắt buộc có điều kiện' trong PP này như sau. 'Các SFR bắt buộc có điều kiện' bắt buộc phải được đưa vào ST, nếu chúng đáp ứng 'các điều kiện bổ sung cho ST' trong bảng bên dưới.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lớp chức năng bảo mật | Thành phần chức năng bảo mật | | Điều kiện bổ sung SFR | Ghi chú |
| FAU | FAU\_STG.1 | Lưu trữ dấu vết kiểm tra được bảo vệ | Trong trường hợp máy chủ TOE lưu trữ các bản ghi kiểm tra trong bộ nhớ cục bộ |  |
| FAU\_STG.3 | Hành động trong trường hợp có thể mất dữ liệu kiểm tra | Trong trường hợp máy chủ TOE lưu trữ các bản ghi kiểm tra trong bộ nhớ cục bộ |  |
| FAU\_STG.4 | Ngăn ngừa mất dữ liệu kiểm tra | Trong trường hợp máy chủ TOE lưu trữ hồ sơ kiểm tra trong bộ nhớ cục bộ |  |
| FIA | FIA\_UAU.5 | Cơ chế đa xác thực Trong trường hợp máy chủ | TOE tự hỗ trợ các chức năng xác thực và nhận dạng bổ sung ngoài phương thức xác thực dựa trên ID/mật khẩu |  |
| FPT | FPT\_ITT.1 | Bảo vệ truyền dữ liệu TSF nội bộ cơ bản | Trong trường hợp TOE được tách biệt về mặt vật lý (ví dụ: máy chủ, bảng điều khiển quản lý, v.v.) |  |
| FPT\_LEE.1 | Các thực thể bên ngoài có thể liên kết (Mở rộng) - xác thực | Trong trường hợp máy chủ TOE hỗ trợ các chức năng xác thực và nhận dạng bổ sung bằng cách tương tác với các thực thể CNTT bên ngoài ngoài phương thức xác thực dựa trên ID/mật khẩu |  |
| FTA | FTA\_SSL.1 | Khóa phiên do TSF khởi tạo | Trong trường hợp TOE cung cấp chức năng khóa phiên | Một trong hai phải được thực hiện |
| FTA\_SSL.3 | Chấm dứt do TSF khởi tạo | Trong trường hợp TOE cung cấp chức năng kết thúc phiên |  |
| FTA\_TSE.1(2) | Thiết lập phiên TOE | Trong trường hợp cần phải xác định và xác thực người dùng hiện có trong tác nhân, bảng điều khiển quản lý hoặc ứng dụng khách cấu thành TOE |  |
| FTP | FTP\_ITC.1 | Kênh tin cậy giữa các TSF | Trong trường hợp tương tác với các thực thể CNTT bên ngoài được hỗ trợ.  Trong trường hợp các bản ghi kiểm toán được truyền và lưu trữ cho các thực thể CNTT bên ngoài trong thời gian thực.  Trong trường hợp cung cấp chức năng cập nhật trực tuyến thông qua máy chủ cập nhật của nhà phát triển. |  |
| FTP\_TRP.1 | Đường dẫn tin cậy | Trong trường hợp quản trị viên được ủy quyền và người dùng chung truy cập trực tiếp vào máy chủ quản lý thông qua trình duyệt web hoặc chương trình truy cập đầu cuối, v.v. |  |

[Bảng 7] Các SFR bắt buộc có điều kiện

1. Kiểm toán bảo mật (FAU)

8.2.1.1. FAU\_STG.1 Lưu trữ dấu vết kiểm tra được bảo vệ

|  |  |
| --- | --- |
| Phân cấp | Không có các thành phần khác |
| Các thành phần | phụ thuộc FAU\_GEN.1 Tạo dữ liệu kiểm tra |
| FAU\_STG.1.1 | TSF sẽ bảo vệ các bản ghi kiểm tra được lưu trữ trong đường kiểm tra khỏi bị xóa trái phép. |
| FAU\_STG.1.2 | TSF phải có khả năng ngăn chặn các sửa đổi trái phép đối với các bản ghi kiểm toán được lưu trữ trong lớp kiểm toán |

|  |
| --- |
| Lưu ý áp dụng  TOE sẽ bảo vệ các bản ghi kiểm tra không bị xóa hoặc thay đổi.  - Một chức năng sẽ được triển khai để lưu trữ hồ sơ kiểm toán trong bộ lưu trữ cục bộ hoặc để truyền và lưu trữ hồ sơ kiểm toán cho một thực thể CNTT bên ngoài trong thời gian thực.  - Các lệnh giao diện người dùng (UI) và CLI có liên quan sẽ không được cung cấp để ngay cả quản trị viên được ủy quyền cũng không thể xóa hoặc thay đổi hồ sơ kiểm toán.  - Việc truy cập của người không được phép sẽ được kiểm soát để bảo vệ hồ sơ kiểm toán được lưu trữ.  - Nếu không thể thực hiện đầy đủ chức năng bảo mật TOE, thì môi trường vận hành TOE có thể hỗ trợ lưu trữ dấu vết kiểm toán được bảo vệ.  • Ví dụ: Khi các bản ghi kiểm toán được lưu trữ trong DBMS được cài đặt trên cùng hệ điều hành với TOE, các chức năng xác thực và nhận dạng của DBMS có thể được sử dụng để bảo vệ việc xóa hoặc sửa đổi bởi người dùng trái phép.  - Nếu hồ sơ kiểm tra được lưu trữ trong máy chủ nhật ký bên ngoài TOE, giao tiếp được mã hóa sẽ được thực hiện.  • Nếu nhật ký hệ thống được hỗ trợ, thì việc truyền mã hóa sẽ được hỗ trợ thông qua *nhật ký hệ thống qua DTLS(RFC 5424), nhật ký hệ thống qua DTLS(RFC 6012), v.v.* |

8.2.1.2. FAU\_STG.3 Hành động trong trường hợp mất dữ liệu kiểm toán

|  |  |
| --- | --- |
| Phân cấp | Không có các thành phần khác |
| Các thành phần phụ thuộc | FAU\_STG.1 Lưu trữ dấu vết kiểm tra được bảo vệ |
| FAU\_STG.3.1 | TSF sẽ [Thông báo cho quản trị viên được ủy quyền, [lựa chọn: *hành động được thực hiện trong trường hợp có thể xảy ra lỗi lưu trữ kiểm tra*] nếu dấu vết kiểm tra vượt quá [lựa chọn: *trước -giới hạn xác định*] |

|  |
| --- |
| Lưu ý áp dụng  Trong trường hợp kích thước của bản ghi kiểm tra đạt đến dung lượng được xác định trước, TOE sẽ thực hiện các hành động phản hồi như thông báo cho quản trị viên.  - Một chức năng sẽ được thực hiện để lưu trữ hồ sơ kiểm tra trong bộ lưu trữ cục bộ hoặc để truyền và lưu trữ hồ sơ kiểm tra cho một thực thể CNTT bên ngoài trong thời gian thực.  - Có chức năng thông báo cho người quản trị. Ví dụ về chức năng như sau.  • Cảnh báo màn hình, gửi email cho quản trị viên, v.v.  - Ví dụ về các điều kiện để thông báo cho quản trị viên về việc mất hồ sơ kiểm toán như sau.  • Dung lượng đĩa cài đặt còn 90% trở lên, 100MB trở lên, v.v.  - Ngoài ra, có thể cung cấp chức năng cho quản trị viên gửi hồ sơ kiểm toán đến máy chủ nhật ký bên ngoài.  • Nếu nhật ký hệ thống được hỗ trợ, thì việc truyền mã hóa sẽ được hỗ trợ thông qua nhật ký hệ thống qua DTLS(RFC 5424), nhật ký hệ thống qua DTLS(RFC 6012), v.v.  • Thuật toán mật mã được sử dụng, bảo mật khóa mật mã và phương pháp lưu trữ khóa mật mã phải đáp ứng 'bảo vệ' khi lưu trữ khóa mật mã' yêu cầu của lớp FCS và FPT\_PST.1. |

8.2.1.3. FAU\_STG.4 Ngăn ngừa mất dữ liệu kiểm tra

|  |  |
| --- | --- |
| Phân cấp | FAU\_STG.3 Hành động trong trường hợp có thể mất dữ liệu kiểm toán |
| Các thành phần phụ thuộc | FAU\_STG.1 Lưu trữ dấu vết kiểm toán được bảo vệ FAU\_STG.4.1 |
|  | TSF phải [lựa chọn, chọn một trong số: *“bỏ qua các sự kiện được kiểm toán”, “ngăn chặn các sự kiện được kiểm toán, ngoại trừ những sự kiện được thực hiện bởi người dùng được ủy quyền có quyền đặc biệt”, “ghi đè lên hồ sơ kiểm tra được lưu trữ cũ nhất*”] và [lựa chọn: *các hành động khác được thực hiện trong trường hợp lỗi lưu trữ kiểm tra*] nếu dấu vết kiểm tra đã đầy |

|  |
| --- |
| Lưu ý áp dụng  Trong trường hợp dung lượng lưu trữ hồ sơ kiểm toán đầy, TOE sẽ phản hồi lỗi không lưu theo cách thích hợp.  - Một chức năng sẽ được triển khai để lưu trữ hồ sơ kiểm toán trong bộ lưu trữ cục bộ hoặc để truyền và lưu trữ hồ sơ kiểm toán cho một thực thể CNTT bên ngoài trong thời gian thực.  - Ví dụ về chức năng phản hồi trong trường hợp không lưu được như sau.  *• Ghi đè các bản ghi kiểm tra cũ nhất, lưu nén các bản ghi kiểm tra, v.v.* |

1. Định danh và xác thực (FIA)

8.2.2.1. FIA\_UAU.5 Nhiều cơ chế xác thực

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Phụ thuộc | Không phụ thuộc |
| FIA\_UAU.5.1 | TSF phải cung cấp [cơ chế xác thực mật khẩu, [lựa chọn: *danh sách cơ chế xác thực bổ sung*]] để hỗ trợ xác thực người dùng. |
| FIA\_UAU.5.2 | TSF sẽ xác thực danh tính được yêu cầu của bất kỳ người dùng nào theo [lựa chọn: *quy tắc mô tả cách thức nhiều cơ chế xác thực cung cấp xác thực*] |

|  |
| --- |
| Lưu ý áp dụng  Trong trường hợp TOE hỗ trợ các phương thức xác thực và nhận dạng bổ sung, TOE sẽ tự cung cấp các chức năng định danh và xác thực bổ sung hoặc bằng cách tương tác với các thực thể CNTT bên ngoài, song song với định danh và xác thực dựa trên tài khoản/mật khẩu người dùng.  - Để cung cấp các chức năng định danh và xác thực bổ sung, có thể sử dụng thiết bị hỗ trợ △2FA tuân thủ các tiêu chuẩn FIDO, △chứng chỉ, △trình tạo mật khẩu dùng một lần (OTP), v.v.  • Nếu nó được hỗ trợ trong môi trường vận hành TOE, nên sử dụng 'thiết bị hỗ trợ 2FA tuân thủ các tiêu chuẩn FIDO'.  - Nếu các chức năng định danh và xác thực bổ sung được cung cấp trong TOE, thì các chức năng này có thể được cung cấp bằng cách nhận kết quả xác thực từ bên trong TOE hoặc từ các thực thể CNTT bên ngoài tương tác.  • Nếu TOE cung cấp phương pháp sử dụng chứng nhận, thì việc xác thực chứng chỉ sẽ được thực hiện.  • Thông tin xác thực được sử dụng bởi các thực thể CNTT bên ngoài để thực hiện các phương pháp xác thực và nhận dạng bổ sung sẽ được quản lý an toàn bởi các thực thể CNTT bên ngoài. Nếu TOE lưu trữ thông tin xác thực được sử dụng để thực hiện các phương thức xác thực và nhận dạng bổ sung, các yêu cầu của FPT\_PST.1 sẽ được áp dụng |

1. Bảo vệ TSF (FPT)

8.2.3.1. FPT\_ITT.1 Bảo vệ truyền dữ liệu TSF nội bộ cơ bản

|  |  |
| --- | --- |
| Phân cấp đến | Phân cấp đến |
| Các thành phần phụ thuộc | Không phụ thuộc. |
| FPT\_ITT.1.1 | TSF sẽ bảo vệ dữ liệu TSF khỏi bị tiết lộ và sửa đổi khi dữ liệu TSF được truyền giữa các phần riêng biệt của TOE. |

|  |
| --- |
| Lưu ý áp dụng  TOE sẽ truyền bằng cách sử dụng kênh được mã hóa để bảo vệ dữ liệu được truyền giữa các thành phần TOE (ví dụ: chính sách bảo mật, lệnh điều khiển, hồ sơ kiểm toán, v.v.)  - Để truyền thông được mã hóa an toàn, tính bảo mật và tính toàn vẹn sẽ được cung cấp bằng các giao thức chuẩn.  • Các giao thức liên lạc mã hóa an toàn bao gồm HTTPS (được triển khai bằng TLS), TLS (TLS 1.2-RFC5246 trở lên), SSH (SSH V2-RFC 4251, 4254), v.v.  - Không được phép sử dụng giao thức riêng.  - Thuật toán mật mã sử dụng, độ bảo mật khóa mật mã và phương thức lưu trữ khóa mật mã phải đáp ứng yêu cầu “bảo vệ khi lưu trữ khóa mật mã” của lớp FCS và FPT\_PST.1. |

8.2.3.2. FPT\_LEE.1 Các thực thể bên ngoài có thể liên kết (Mở rộng) - xác thực

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| FPT\_LEE.1.1 | TSF sẽ thực hiện [lựa chọn: danh sách các hành động] và cung cấp [lựa chọn: danh sách các chức năng] bằng cách liên kết với các thực thể bên ngoài |

|  |
| --- |
| Lưu ý áp dụng  Trong trường hợp TOE hỗ trợ các phương thức xác thực và nhận dạng bổ sung, TOE sẽ tự cung cấp các chức năng định danh và xác thực bổ sung hoặc bằng cách tương tác với các thực thể CNTT bên ngoài, song song với định danh và xác thực dựa trên tài khoản/mật khẩu người dùng.  - Để cung cấp các chức năng định danh và xác thực bổ sung, có thể sử dụng thiết bị hỗ trợ △2FA tuân thủ các tiêu chuẩn FIDO, △chứng chỉ, △trình tạo mật khẩu dùng một lần (OTP), v.v.  • Nếu nó được hỗ trợ trong môi trường vận hành TOE, nên sử dụng 'thiết bị hỗ trợ 2FA tuân thủ các tiêu chuẩn FIDO'.  - Nếu các chức năng định danh và xác thực bổ sung được cung cấp trong TOE, thì các chức năng này có thể được cung cấp bằng cách nhận kết quả xác thực từ bên trong TOE hoặc từ các thực thể CNTT bên ngoài tương tác.  • Nếu TOE cung cấp phương pháp sử dụng chứng nhận, thì việc xác thực chứng chỉ sẽ được thực hiện.  • Thông tin xác thực được sử dụng bởi các thực thể CNTT bên ngoài để thực hiện các phương pháp xác thực và nhận dạng bổ sung sẽ được quản lý an toàn bởi các thực thể CNTT bên ngoài. Nếu TOE lưu trữ thông tin xác thực được sử dụng để thực hiện các phương thức xác thực và nhận dạng bổ sung, các yêu cầu của FPT\_PST.1 sẽ được áp dụng |

1. Truy cập TOE (FTA)

8.2.4.1. Khóa phiên do TSF khởi tạo FTA\_SSL.1

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | FIA\_UAU.1 Thời gian xác thực |
| FTA\_SSL.1.1 | TSF sẽ khóa phiên tương tác sau [lựa chọn: *khoảng thời gian người dùng không hoạt động*] bằng cách:  a) xóa hoặc ghi đè thiết bị hiển thị, làm cho nội dung hiện tại không thể đọc được;  b) vô hiệu hóa bất kỳ hoạt động nào của thiết bị hiển thị/truy cập dữ liệu của người dùng ngoài việc mở khóa phiên. |
| FTA\_SSL.1.2 | TSF sẽ yêu cầu các sự kiện sau xảy ra trước khi mở khóa phiên: [ [lựa chọn: *mở khóa phiên bởi quản trị viên, xác thực lại người dùng trước khi mở khóa phiên*] ] |

|  |
| --- |
| Lưu ý áp dụng  TOE sẽ cung cấp chức năng khóa hoặc chấm dứt phiên nếu nó không được sử dụng trong một khoảng thời gian nhất định sau khi phiên người dùng được kết nối.  - Thông tin thời gian được sử dụng sẽ được áp dụng dựa trên thời gian của máy chủ.  - Một khoảng thời gian nhất định đề cập đến lượng thời gian tích lũy sau khi kết nối kích hoạt khóa phiên hoặc chấm dứt.  • Quản trị viên có thể cố định một khoảng thời gian nhất định trong khoảng 10 phút hoặc ít hơn hoặc đặt tương ứng với số lần xác thực không thành công.  - Sau khi hết thời gian khóa, phiên bị khóa sẽ được mở khóa bởi người quản trị hoặc thông qua chức năng xác thực người dùng cho từng phiên. - Một bản ghi kiểm toán sẽ được tạo khi khóa phiên hoặc chức năng kết thúc được kích hoạt.  - Nó sẽ được áp dụng cho tất cả quản lý và truy cập cục bộ có trong TOE. |

8.2.4.2. FTA\_SSL.3 Chấm dứt do TSF khởi tạo

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| FTA\_SSL.3.1 | TSF sẽ kết thúc phiên tương tác sau [lựa chọn: khoảng thời gian người dùng không hoạt động] |

|  |
| --- |
| Lưu ý áp dụng  TOE sẽ cung cấp chức năng khóa hoặc chấm dứt phiên nếu nó không được sử dụng cho khoảng thời gian nhất định sau khi phiên người dùng được kết nối.  - Thông tin thời gian được sử dụng sẽ được áp dụng dựa trên thời gian của máy chủ.  - Một khoảng thời gian nhất định đề cập đến lượng thời gian tích lũy sau khi kết nối kích hoạt khóa phiên hoặc chấm dứt.  • Quản trị viên có thể cố định một khoảng thời gian nhất định trong khoảng 10 phút hoặc ít hơn hoặc đặt tương ứng với số lần xác thực không thành công.  - Sau khi hết thời gian khóa, phiên bị khóa sẽ được mở khóa bởi người quản trị hoặc thông qua chức năng xác thực người dùng cho từng phiên.  - Một bản ghi kiểm toán sẽ được tạo khi khóa phiên hoặc chức năng kết thúc được kích hoạt.  - Nó sẽ được áp dụng cho tất cả quản lý và truy cập cục bộ có trong TOE |

5.2.4.3. FTA\_TSE.1(2) Thiết lập phiên TOE

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| FTA\_TSE.1.1 | TSF sẽ có thể từ chối việc thiết lập phiên dựa trên [lựa chọn: danh sách các thuộc tính bổ sung của tác nhân hoặc khách hàng.] |

|  |
| --- |
| Lưu ý áp dụng  Trong trường hợp cần xác định và xác thực người dùng tồn tại trong đại lý hoặc khách hàng cấu thành TOE, giá trị nhận dạng sẽ là một giá trị duy nhất không được đăng ký trùng lặp.  - Trong quá trình xác thực người dùng, các thuộc tính bổ sung của đại lý hoặc khách hàng đã đăng ký cũng sẽ được xác thực.  - Các thuộc tính bổ sung: Địa chỉ IP là bắt buộc và ít nhất một trong số *địa chỉ MAC, số sê-ri và thông tin có thể xác định duy nhất chính tác nhân đó* sẽ được sử dụng bổ sung. |

1. Đường dẫn/kênh tin cậy (FTP)

8.2.5.1. FTP\_ITC.1 Kênh tin cậy giữa các TSF

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| FTP\_ITC.1.1 | TSF sẽ cung cấp một kênh liên lạc giữa chính nó và một sản phẩm CNTT đáng tin cậy khác, khác biệt về mặt logic với các kênh liên lạc khác và cung cấp sự xác định chắc chắn về các điểm cuối và bảo vệ dữ liệu kênh khỏi bị sửa đổi hoặc tiết lộ. |
| FTP\_ITC.1.2 | TSF phải cho phép [lựa chọn: TSF, một sản phẩm CNTT tin cậy khác] bắt đầu truyền thông qua kênh tin cậy. |
| FTP\_ITC.1.3 | TSF sẽ bắt đầu truyền thông qua kênh tin cậy cho [lựa chọn: danh sách các chức năng mà kênh tin cậy được yêu cầu] |

|  |
| --- |
| Lưu ý áp dụng  Trong trường hợp tương tác với các thực thể CNTT bên ngoài được hỗ trợ, TOE sẽ truyền dữ liệu bằng kênh liên lạc được mã hóa để bảo vệ dữ liệu được truyền khi tương tác với các thực thể CNTT bên ngoài.  - Để liên lạc bằng mật mã an toàn, tính bảo mật và tính toàn vẹn phải được cung cấp bằng cách sử dụng các giao thức tiêu chuẩn.  • Các giao thức liên lạc mã hóa an toàn bao gồm HTTPS (được triển khai bằng TLS), TLS (TLS 1.2-RFC5246 trở lên), SSH (SSH V2-RFC 4251, 4254), v.v.  - Không được phép sử dụng giao thức riêng. - Kênh liên lạc mật mã có thể được triển khai trực tiếp trong TOE hoặc được cung cấp bởi TOE bằng cách sử dụng môi trường vận hành.  - Yêu cầu này sẽ được áp dụng khi TOE cung cấp chức năng tương tác với các thực thể CNTT bên ngoài để cung cấp chức năng bảo mật.  - Nếu dữ liệu truyền không được bảo vệ bằng kênh liên lạc mật mã khi tương tác với các thực thể CNTT bên ngoài, thì sự cần thiết phải bảo vệ tính bảo mật và tính toàn vẹn của dữ liệu được truyền sẽ được chứng minh.  - Các dịch vụ liên lạc không hỗ trợ các kênh liên lạc mật mã sẽ có thể bị vô hiệu hóa.  - Thuật toán mật mã sử dụng, độ bảo mật khóa mật mã và phương thức lưu trữ khóa mật mã phải đáp ứng yêu cầu “bảo vệ khi lưu trữ khóa mật mã” của lớp FCS và FPT\_PST.1. Trong trường hợp hồ sơ kiểm toán được lưu trữ trong máy chủ nhật ký bên ngoài TOE, giao tiếp bằng mật mã sẽ được thực hiện.  - Nếu nhật ký hệ thống được hỗ trợ, thì việc truyền mã hóa sẽ được hỗ trợ thông qua nhật ký hệ thống qua DTLS(RFC 5424), nhật ký hệ thống qua DTLS(RFC 6012), v.v. |

8.2.5.2. FTP\_TRP.1 Đường dẫn đáng tin cậy

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| FTP\_TRP.1.1 | TSF sẽ cung cấp một đường giao tiếp giữa chính nó và những người dùng [lựa chọn: từ xa, cục bộ] khác biệt về mặt logic với các đường giao tiếp khác và cung cấp sự xác định chắc chắn các điểm cuối của nó và bảo vệ các dữ liệu được truyền đạt từ *việc sửa đổi, tiết lộ, [lựa chọn: các loại vi phạm tính toàn vẹn hoặc bảo mật khác].* |
| FTP\_TRP.1.2 | TSF phải cho phép [lựa chọn: *TSF, người dùng cục bộ, người dùng từ xa*] bắt đầu giao tiếp qua đường dẫn tin cậy. |
| FTP\_TRP.1.3 | TSF sẽ yêu cầu sử dụng đường dẫn tin cậy cho [lựa chọn: ***xác thực quản trị viên truy cập quản lý***, [lựa chọn: *các dịch vụ khác cần có đường dẫn tin cậy*] ] |

|  |
| --- |
| Lưu ý áp dụng  Trong quá trình truy cập quản lý, TOE sẽ truyền dữ liệu bằng cách sử dụng kênh liên lạc mật mã để bảo vệ dữ liệu được truyền.  - Để liên lạc bằng mật mã an toàn, tính bảo mật và tính toàn vẹn phải được cung cấp bằng cách sử dụng các giao thức tiêu chuẩn.  • Các giao thức liên lạc mã hóa an toàn bao gồm HTTPS (được triển khai bằng TLS), TLS (TLS 1.2-RFC5246 trở lên), SSH (SSH V2-RFC 4251, 4254), v.v.  - Không được phép sử dụng giao thức riêng.  - Kênh truyền thông mật mã có thể được triển khai trực tiếp trong TOE hoặc được TOE cung cấp bằng cách sử dụng môi trường vận hành.  - Thuật toán mật mã sử dụng, độ bảo mật khóa mật mã và phương thức lưu trữ khóa mật mã phải đáp ứng yêu cầu “bảo vệ khi lưu trữ khóa mật mã” của lớp FCS và FPT\_PST.1. |

Yêu cầu chức năng an toàn (SFR tùy chọn)

'SFR tùy chọn' trong PP này như sau. Các 'SFR tùy chọn' không bắt buộc phải được triển khai một cách bắt buộc, nhưng nếu TOE cung cấp thêm các chức năng liên quan, Người yêu cầu đánh giá sẽ bao gồm các SFR tương ứng trong ST

|  |  |  |
| --- | --- | --- |
| Lớp chức năng bảo mật | Thành phần chức năng bảo mật | |
| Hỗ trợ mật mã (FCS) | FCS\_CKM.2 | Phân phối khóa mật mã |
| Bảo vệ TSF (FPT) | FPT\_STM.1 | Dấu thời gian đáng tin cậy |

[Bảng 8] Các SFR tùy chọn

1. Hỗ trợ mật mã (FCS)

8.3.1.1. FCS-CKM.2 Phân phối khóa mật mã

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | [FDP\_ITC.1 Nhập dữ liệu người dùng không có thuộc tính bảo mật hoặc  FDP\_ITC.2 Nhập dữ liệu người dùng có thuộc tính bảo mật hoặc  FCS\_CKM.1 Tạo khóa mật mã] FCS\_CKM.4 Phá hủy khóa mật mã |
| FCS\_CKM.2.1 | TSF sẽ phân phối khóa mật mã theo với một phương thức phân phối khóa mật mã được lựa chọn [lựa chọn: *phương pháp phân phối khóa mật mã*] đáp ứng những điều sau: [lựa chọn: *danh sách các tiêu chuẩn*] |

|  |
| --- |
| Lưu ý áp dụng  Phân phối khóa mật mã FCS\_CKM.2 là một yêu cầu chức năng có thể triển khai có chọn lọc ('SFR tùy chọn') và nếu TOE cung cấp thêm chức năng trên, Người yêu cầu đánh giá sẽ đưa yêu cầu này vào SFR.  Nếu Người yêu cầu đánh giá bao gồm SFR này, thì định nghĩa vấn đề an toàn và các mục tiêu an toàn sẽ được đưa ra bổ sung, nếu cần.  Khóa được sử dụng trong phương thức thiết lập khóa mật mã được xác định trong FCS\_CKM.2.1 phải liên quan đến khóa được tạo trong FCS\_CKM.1.1 của FCS\_CKM.1 |

1. Bảo vệ TSF (FPT)

8.3.2.1. FPT\_STM.1 Dấu thời gian đáng tin cậy

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| FTP\_STM.1.1 | TSF sẽ có thể cung cấp dấu thời gian đáng tin cậy |

|  |
| --- |
| Lưu ý áp dụng  Mỗi thành phần của TOE sẽ tạo hồ sơ kiểm tra bằng cách sử dụng thông tin thời gian đáng tin cậy.  - Thông tin về thời gian tin cậy sẽ sử dụng thông tin về thời gian do máy chủ NTP hoặc hệ điều hành cung cấp.. |

* 1. Yêu cầu đảm bảo an toàn

Các yêu cầu đảm bảo của Hồ sơ bảo vệ này bao gồm các thành phần đảm bảo trong CC phần 3 và mức đảm bảo đánh giá là EAL1+. Bảng dưới đây tóm tắt các thành phần đảm bảo

|  |  |  |
| --- | --- | --- |
| Lớp đảm bảo an toàn | Thành phần đảm bảo an toàn | |
| Bảo mật Đánh giá mục tiêu | ASE\_INT.1 | Giới thiệu ST |
| ASE\_CCL.1 | Các Yêu cầu tuân thủ |
| ASE\_OBJ.1 | Các mục tiêu an toàn cho môi trường vận hành |
| ASE\_ECD.1 | Định nghĩa các thành phần mở rộng |
| ASE\_REQ.1 | Các yêu cầu an toàn đã nêu |
| ASE\_TSS.1 | Đặc tả tóm tắt TOE |
| Phát triển | ADV\_FSP.1 | Đặc tả chức năng cơ bản |
| Tài liệu hướng dẫn | AGD\_OPE.1 | Hướng dẫn người dùng vận hành |
| AGD\_PRE.1 | Quy trình chuẩn bị |
| Hỗ trợ vòng đời | ALC\_CMC.1 | Gắn nhãn cho TOE |
| ALC\_CMS.1 | Phạm vi TOE CM |
| Thử nghiệm | ATE\_FUN.1 | Thử nghiệm chức năng |
| ATE\_IND.1 | Thử nghiệm độc lập - tuân thủ |
| Đánh giá lỗ hổng | AVA\_VAN.1 | Khảo sát lỗ hổng |

[Bảng 9] Yêu cầu đảm bảo an toàn

1. Bảo mật Đánh giá mục tiêu

9.1.1 Giới thiệu ASE\_INT.1 ST

|  |  |
| --- | --- |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| Các yếu tố hành động của nhà phát triển |  |
| ASE\_INT.1.1D | Các yếu tố hành động của nhà phát triển |
| Các thành phần nội dung và trình bày |  |
| ASE\_INT.1.1C | Phần giới thiệu ST sẽ bao gồm tham chiếu ST, tham chiếu TOE, tổng quan TOE và mô tả TOE. |
| ASE\_INT.1.2C | Tham chiếu ST sẽ xác định duy nhất ST. |
| ASE\_INT.1.3C | Tham chiếu TOE sẽ xác định duy nhất TOE. |
| ASE\_INT.1.4C | Tổng quan về TOE sẽ tóm tắt cách sử dụng và các tính năng bảo mật chính của TOE. |
| ASE\_INT.1.5C | Tổng quan TOE sẽ xác định loại TOE. |
| ASE\_INT.1.6C | Tổng quan về TOE sẽ xác định bất kỳ phần cứng/phần mềm/phần sụn không phải TOE nào được yêu cầu bởi TOE. |
| ASE\_INT.1.7C | Mô tả TOE sẽ mô tả phạm vi vật lý của TOE. |
| ASE\_INT.1.8C | Mô tả TOE sẽ mô tả phạm vi logic của TOE. |
| Các yếu tố hành động của người đánh giá |  |
| ASE\_INT.1.1E | Người đánh giá phải xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và cách trình bày bằng chứng. |
| ASE\_INT.1.2E | Người đánh giá phải xác nhận rằng tham chiếu TOE, tổng quan TOE và mô tả TOE nhất quán với nhau |

9.1.2. ASE\_CCL.1 Yêu cầu tuân thủ

|  |  |
| --- | --- |
| Các thành phần phụ thuộc |  |
| ASE\_INT.1 | Giới thiệu ST |
| ASE\_ECD.1 | Định nghĩa các thành phần mở rộng |
| ASE\_REQ.1 | Các yêu cầu bảo mật đã nêu |
| Các yếu tố hành động của nhà phát triển |  |
| ASE\_CCL.1.1D | Nhà phát triển sẽ cung cấp yêu cầu tuân thủ. |
| ASE\_CCL.1.2D | Nhà phát triển phải cung cấp cơ sở cho yêu cầu tuân thủ |
| Các phần tử nội dung và trình bày |  |
| ASE\_CCL.1.1C | Yêu cầu tuân thủ sẽ chứa một yêu cầu tuân thủ |
| ASE\_CCL.1.2C | Yêu cầu tuân thủ CC sẽ mô tả sự tuân thủ của ST với CC Phần 2 là tuân thủ CC Phần 2 hoặc CC Phần 2 mở rộng |
| ASE\_CCL.1.3C | Yêu cầu tuân thủ CC sẽ mô tả sự tuân thủ của ST với CC Phần 3 là tuân thủ CC Phần 3 hoặc CC Phần 3 mở rộng |
| ASE\_CCL.1.4C | Yêu cầu tuân thủ CC phải phù hợp với định nghĩa thành phần mở rộng. |
| ASE\_CCL.1.5C | Yêu cầu tuân thủ sẽ xác định tất cả các PP và gói yêu cầu bảo mật mà ST yêu cầu tuân thủ |
| ASE\_CCL.1.6C | Yêu cầu tuân thủ sẽ mô tả bất kỳ sự tuân thủ nào của ST đối với gói dưới dạng gói tuân thủ hoặc gói được tăng cường. |
| ASE\_CCL.1.7C | Cơ sở lý luận về yêu cầu tuân thủ phải chứng minh rằng loại TOE nhất quán với loại TOE trong PP mà sự tuân thủ đang được yêu cầu. |
| ASE\_CCL.1.8C | Cơ sở lý luận của yêu cầu tuân thủ phải chứng minh rằng tuyên bố về định nghĩa vấn đề an toàn nhất quán với tuyên bố về định nghĩa vấn đề an toàn trong các PP mà theo đó sự tuân thủ đang được yêu cầu. |
| ASE\_CCL.1.9C | Cơ sở lý luận về yêu cầu tuân thủ phải chứng minh rằng tuyên bố về các mục tiêu bảo mật nhất quán với tuyên bố về các mục tiêu bảo mật trong PP mà theo đó sự tuân thủ đang được yêu cầu. |
| ASE\_CCL.1.10C | Cơ sở lý luận về yêu cầu tuân thủ sẽ chứng minh rằng tuyên bố về các yêu cầu bảo mật nhất quán với tuyên bố về các yêu cầu bảo mật trong PP mà theo đó sự tuân thủ đang được yêu cầu |
| Các yếu tố hành động của người đánh giá |  |
| ASE\_CCL.1.1E | Người đánh giá phải xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày bằng chứng |

9.1.3. ASE\_OBJ.1 Mục tiêu bảo mật cho môi trường hoạt động

|  |  |
| --- | --- |
| Các thành phần phụ thuộc | Không phụ thuộc |
| Các yếu tố hành động của nhà phát triển |  |
| ASE\_OBJ.1.1D | Nhà phát triển phải cung cấp tuyên bố về các mục tiêu bảo mật. |
| Các phần tử nội dung và trình bày |  |
| ASE\_OBJ.1.1C | Tuyên bố về các mục tiêu an toàn sẽ mô tả các mục tiêu an toàn cho môi trường vận hành. |
| Các yếu tố hành động của người đánh giá |  |
| ASE\_OBJ.1.1E | Người đánh giá phải xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và cách trình bày bằng chứng. |

9.1.4. ASE\_ECD.1 Định nghĩa thành phần mở rộng

|  |  |
| --- | --- |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| Các yếu tố hành động của nhà phát triển |  |
| ASE\_ECD.1.1D | Nhà phát triển sẽ cung cấp một tuyên bố về các yêu cầu bảo mật. |
| ASE\_ECD.1.2D | Nhà phát triển sẽ cung cấp định nghĩa thành phần mở rộng |
| Các yếu tố nội dung và trình bày |  |
| ASE\_ECD.1.1C | Tuyên bố về các yêu cầu bảo mật sẽ xác định tất cả các yêu cầu bảo mật mở rộng. |
| ASE\_ECD.1.2C | Định nghĩa thành phần mở rộng sẽ xác định thành phần mở rộng cho từng yêu cầu bảo mật mở rộng. |
| ASE\_ECD.1.3C | Định nghĩa các thành phần mở rộng sẽ mô tả cách mỗi thành phần mở rộng liên quan đến các thành phần, họ và lớp CC hiện có. |
| ASE\_ECD.1.4C | Định nghĩa các thành phần mở rộng sẽ sử dụng các thành phần, họ, lớp và phương pháp CC hiện có làm mô hình để trình bày. |
| ASE\_ECD.1.5C | Các thành phần mở rộng sẽ bao gồm các phần tử khách quan và đo lường được sao cho có thể chứng minh sự phù hợp hoặc không phù hợp với các phần tử này |
| Các yếu tố hành động của người đánh giá |  |
| ASE\_ECD.1.1E | Người đánh giá phải xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và cách trình bày bằng chứng. |
| ASE\_ECD.1.2E | Người đánh giá phải xác nhận rằng không có thành phần mở rộng nào có thể được thể hiện rõ ràng bằng cách sử dụng các thành phần hiện có |

9.1.5. ASE\_REQ.1 Các yêu cầu bảo mật đã nêu

|  |  |
| --- | --- |
| Các thành phần phụ thuộc |  |
| ASE\_ECD.1 | Định nghĩa các thành phần mở rộng Các phần tử hành động của nhà phát triển |
| ASE\_REQ.1.1D | Nhà phát triển phải cung cấp một tuyên bố về các yêu cầu bảo mật. |
| ASE\_REQ.1.2D | Nhà phát triển phải cung cấp cơ sở hợp lý cho các yêu cầu bảo mật. Các phần tử nội dung và trình bày |
| ASE\_REQ.1.1C | Tuyên bố về các yêu cầu an toàn sẽ mô tả các SFR và SAR. |
| ASE\_REQ.1.2C | Tất cả các chủ thể, đối tượng, hoạt động, thuộc tính bảo mật, thực thể bên ngoài và các thuật ngữ khác được sử dụng trong SFR và SAR sẽ được xác định. |
| ASE\_REQ.1.3C | Tuyên bố về các yêu cầu bảo mật sẽ xác định tất cả các hoạt động trên các yêu cầu bảo mật. |
| ASE\_REQ.1.4C | Tất cả các hoạt động sẽ được thực hiện một cách chính xác. |
| ASE\_REQ.1.5C | Mỗi sự phụ thuộc của các yêu cầu an toàn phải được thỏa mãn hoặc cơ sở hợp lý của các yêu cầu an toàn sẽ biện minh cho sự phụ thuộc không được thỏa mãn. |
| ASE\_REQ.1.6C | Tuyên bố về các yêu cầu bảo mật phải nhất quán nội bộ. hành động của người đánh giá |
| Các yếu tố hành động của người đánh giá |  |
| ASE\_REQ.1.1E | Người đánh giá phải xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày bằng chứng |

9.1.6. Đặc tả tóm tắt ASE\_TSS.1 TOE

|  |  |
| --- | --- |
| Các thành phần phụ thuộc |  |
| ASE\_INT.1 | Giới thiệu ST |
| ASE\_REQ.1 | Các yêu cầu bảo mật đã nêu |
| ADV\_FSP.1 | Đặc tả chức năng cơ bản |
| Các phần tử hành động của nhà phát triển |  |
| ASE\_TSS.1.1D | Nhà phát triển phải cung cấp một đặc tả tóm tắt TOE |
| Các yếu tố hành động của người đánh giá |  |
| ASE\_TSS.1.1C | Đặc tả tóm tắt TOE sẽ mô tả cách TOE đáp ứng từng SFR. |
| Các yếu tố hành động của người đánh giá |  |
| ASE\_TSS.1.1E | Người đánh giá phải xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và cách trình bày bằng chứng. |
| ASE\_TSS.1.2E | Người đánh giá phải xác nhận rằng đặc tả tóm tắt TOE nhất quán với tổng quan TOE và mô tả TOE |

9.2. Phát triển

9.2.1. ADV\_FSP.1 Đặc tả chức năng cơ bản

|  |  |
| --- | --- |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| Các phần tử hành động của nhà phát triển |  |
| ADV\_FSP.1.1D | Nhà phát triển sẽ cung cấp một đặc tả chức năng. |
| ADV\_FSP.1.2D | Nhà phát triển sẽ cung cấp một dấu vết từ đặc tả chức năng đến các SFR. |
| Các phần tử nội dung và trình bày |  |
| ADV\_FSP.1.1C | Đặc tả chức năng sẽ mô tả mục đích và phương pháp sử dụng cho mỗi TSFI thực thi SFR và hỗ trợ SFR. |
| ADV\_FSP.1.2C | Đặc tả chức năng sẽ xác định tất cả các tham số được liên kết với từng TSFI thực thi SFR và hỗ trợ SFR. |
| ADV\_FSP.1.3C | Đặc tả chức năng sẽ cung cấp cơ sở hợp lý cho việc phân loại ngầm định các giao diện là không can thiệp SFR. |
| ADV\_FSP.1.4C | Việc theo dõi phải chứng minh rằng các SFR theo dõi tới các TSFI trong đặc tả chức năng |
| Các yếu tố hành động của người đánh giá |  |
| ADV\_FSP.1.1E | Người đánh giá phải xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và cách trình bày bằng chứng. |
| ADV\_FSP.1.2E | Người đánh giá phải xác định rằng đặc tả chức năng là một khởi tạo chính xác và đầy đủ của các SFR |

9.3. Tài liệu hướng dẫn

9.3.1. AGD\_OPE.1 Hướng dẫn sử dụng vận hành

|  |  |
| --- | --- |
| Các thành phần phụ thuộc |  |
| ADV\_FSP.1 | Đặc tả chức năng cơ bản |
| Các yếu tố hành động của nhà phát triển |  |
| AGD\_OPE.1.1D | Nhà phát triển sẽ cung cấp hướng dẫn người dùng vận hành. |
| Các thành phần nội dung và trình bày |  |
| AGD\_OPE.1.1C | Hướng dẫn người dùng vận hành sẽ mô tả, đối với từng vai trò người dùng, các chức năng và đặc quyền mà người dùng có thể truy cập cần được kiểm soát trong môi trường xử lý an toàn, bao gồm các cảnh báo thích hợp. |
| AGD\_OPE.1.2C | Hướng dẫn người dùng vận hành sẽ mô tả, đối với từng vai trò người dùng, cách sử dụng các giao diện có sẵn do TOE cung cấp một cách an toàn. |
| AGD\_OPE.1.3C | Hướng dẫn người dùng vận hành sẽ mô tả, đối với từng vai trò người dùng, các chức năng và giao diện có sẵn, đặc biệt là tất cả các tham số bảo mật dưới sự kiểm soát của người dùng, chỉ ra các giá trị bảo mật phù hợp |
| AGD\_OPE.1.4C | Hướng dẫn người dùng vận hành phải, đối với từng vai trò người dùng, trình bày rõ ràng từng loại sự kiện liên quan đến an toàn liên quan đến các chức năng mà người dùng có thể truy cập cần được thực hiện, bao gồm thay đổi các đặc tính an toàn của các thực thể dưới sự kiểm soát của TSF . |
| AGD\_OPE.1.5C | Hướng dẫn người dùng vận hành sẽ xác định tất cả các chế độ vận hành có thể có của TOE (bao gồm vận hành sau lỗi hoặc lỗi vận hành), hậu quả và tác động của chúng đối với việc duy trì vận hành an toàn. |
| AGD\_OPE.1.6C | Hướng dẫn người dùng vận hành sẽ, đối với từng vai trò người dùng, mô tả các biện pháp an toàn cần tuân thủ để hoàn thành các mục tiêu an toàn cho môi trường vận hành như được mô tả trong ST. |
| AGD\_OPE.1.7C | Hướng dẫn sử dụng vận hành phải rõ ràng và hợp lý |
| Các yếu tố hành động của người đánh giá |  |
| AGD\_OPE.1.1E | Người đánh giá phải xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và cách trình bày bằng chứng. |

9.3.2. AGD\_PRE.1 Quy trình chuẩn bị

|  |  |
| --- | --- |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| Các yếu tố hành động của nhà phát triển |  |
| AGD\_PRE.1.1D | Nhà phát triển phải cung cấp TOE bao gồm các thủ tục chuẩn bị của nó. |
| Các yếu tố nội dung và trình bày |  |
| AGD\_PRE1.1C | Các thủ tục chuẩn bị sẽ mô tả tất cả các bước cần thiết để chấp nhận an toàn TOE được chuyển giao theo các thủ tục chuyển giao của nhà phát triển. |
| AGD\_PRE1.2C | Các quy trình chuẩn bị sẽ mô tả tất cả các bước cần thiết để cài đặt an toàn TOE và để chuẩn bị an toàn cho môi trường vận hành theo các mục tiêu an toàn cho môi trường vận hành như được mô tả trong ST. |
| Các yếu tố hành động của người đánh giá |  |
| AGD\_PRE.1.1E | Người đánh giá phải xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và cách trình bày bằng chứng. |
| AGD\_PRE.1.2E | Người đánh giá phải áp dụng các quy trình chuẩn bị để xác nhận rằng TOE có thể được chuẩn bị an toàn để vận hành |

9.4. Hỗ trợ vòng đời

9.4.1. ALC\_CMC.1 Dán nhãn cho TOE

|  |  |
| --- | --- |
| Các thành phần phụ thuộc |  |
| ALC\_CMS.1 | Phạm vi TOE CM |
| Các yếu tố hành động của nhà phát triển |  |
| ALC\_CMC.1.1D | Nhà phát triển sẽ cung cấp TOE và tham chiếu cho TOE. |
| Các phần tử nội dung và trình bày |  |
| ALC\_CMC.1.1C | TOE sẽ được gắn nhãn với tham chiếu duy nhất của nó. |
| Các yếu tố hành động của người đánh giá |  |
| ALC\_CMC.1.1E | Người đánh giá phải xác nhận rằng thông tin được cung cấp đáp ứng các yêu cầu về nội dung và cách trình bày bằng chứng |

9.4.2. Phạm vi ALC\_CMS.1 TOE CM

|  |  |
| --- | --- |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| Các yếu tố hành động của nhà phát triển |  |
| ALC\_CMS.1.1D | Nhà phát triển sẽ cung cấp một danh sách cấu hình cho TOE. |
| Các thành phần nội dung và trình bày |  |
| ALC\_CMS.1.1C | Danh sách cấu hình sẽ bao gồm những điều sau: bản thân TOE; và bằng chứng đánh giá theo yêu cầu của SAR. |
| ALC\_CMS.1.2C | Danh sách cấu hình sẽ xác định duy nhất các mục cấu hình. |
| Các yếu tố hành động của người đánh giá |  |
| ALC\_CMS.1.1E | Người đánh giá phải xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày bằng chứng |

9.5. Thử nghiệm

9.5.1. ATE\_FUN.1 Kiểm tra chức năng

|  |  |
| --- | --- |
| Các thành phần phụ thuộc |  |
| ATE\_COV.1 | Bằng chứng về phạm vi bảo hiểm Các yếu tố hành động của nhà phát triển |
| ATE\_FUN.1.1D | Nhà phát triển phải kiểm tra TSF và ghi lại các kết quả. |
| ATE\_FUN.1.2D | Nhà phát triển sẽ cung cấp tài liệu kiểm tra. |
| Các yếu tố nội dung và trình bày |  |
| ATE\_FUN.1.1C | Tài liệu kiểm thử sẽ bao gồm kế hoạch kiểm thử, kết quả kiểm thử dự kiến ​​và kết quả kiểm thử thực tế |
| ATE\_FUN.1.2C | Các kế hoạch kiểm thử sẽ xác định các kiểm thử sẽ được thực hiện và mô tả các kịch bản để thực hiện từng kiểm thử. Các kịch bản này sẽ bao gồm bất kỳ sự phụ thuộc thứ tự nào vào kết quả của các thử nghiệm khác. |
| ATE\_FUN.1.3C | Kết quả kiểm tra dự kiến sẽ hiển thị kết quả đầu ra dự kiến từ việc thực hiện thành công các kiểm tra. |
| ATE\_FUN.1.4C | Kết quả kiểm tra thực tế phải phù hợp với kết quả kiểm tra dự kiến. |
| Các yếu tố hành động của người đánh giá |  |
| ATE\_FUN.1.1E | Người đánh giá phải xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và trình bày bằng chứng |

9.5.2. ATE\_IND.1 Thử nghiệm độc lập - tuân thủ

|  |  |
| --- | --- |
| Các thành phần phụ thuộc |  |
| ADV\_FSP.1 | Đặc tả chức năng cơ bản |
| AGD\_OPE.1 | Hướng dẫn người dùng vận hành |
| AGD\_PRE.1 | Quy trình chuẩn bị |
| Các yếu tố hành động của nhà phát triển |  |
| ATE\_IND.1.1D | Nhà phát triển phải cung cấp TOE để kiểm tra. |
| Các thành phần nội dung và trình bày |  |
| ATE\_IND.1.1C | TOE phải phù hợp để kiểm thử |
| Các yếu tố hành động của người đánh giá |  |
| ATE\_IND.1.1E | Người đánh giá phải xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và cách trình bày bằng chứng. |
| ATE\_IND.1.2E | Người đánh giá phải kiểm tra một tập hợp con của TSF để xác nhận rằng TSF hoạt động như đã lựa chọn |

9.6. Đánh giá lỗ hổng

9.6.1. Khảo sát lỗ hổng AVA\_VAN.1

|  |  |
| --- | --- |
| Các thành phần phụ thuộc |  |
| ADV\_FSP.1 | Đặc tả chức năng cơ bản AGD\_OPE.1 |
| Hướng dẫn người dùng vận hành |  |
| AGD\_PRE.1 | Quy trình chuẩn bị |
| Các yếu tố hành động của nhà phát triển |  |
| AVA\_VAN.1.1D | Nhà phát triển phải cung cấp TOE để kiểm tra |
| Các yếu tố nội dung và trình bày |  |
| AVA\_VAN.1.1C | TOE phải phù hợp để kiểm tra |
| Các yếu tố hành động của người đánh giá |  |
| AVA\_VAN.1.1E | Người đánh giá phải xác nhận rằng thông tin được cung cấp đáp ứng tất cả các yêu cầu về nội dung và cách trình bày bằng chứng. |
| AVA\_VAN.1.2E | Người đánh giá sẽ thực hiện tìm kiếm các nguồn miền công cộng để xác định các lỗ hổng tiềm ẩn trong TOE. |
| AVA\_VAN.1.3E | Người đánh giá sẽ tiến hành kiểm tra thâm nhập, dựa trên các lỗ hổng tiềm ẩn đã xác định, để xác định rằng TOE có khả năng chống lại các cuộc tấn công do kẻ tấn công có tiềm năng tấn công Cơ bản thực hiện. |

**Phụ lục**

**(Quy định)  
Các định nghĩa thành phần mở rộng**

1. Hỗ trợ mật mã

1.1. Tạo bit ngẫu nhiên

Họ hành vi

Họ này xác định các yêu cầu đối với TSF để cung cấp khả năng tạo ra các bit ngẫu nhiên cần thiết cho hoạt động mã hóa TOE.

Cân bằng các thành phần

1

FCS\_RBG Tạo bit ngẫu nhiên

Tạo bit ngẫu nhiên FCS\_RBG.1, yêu cầu TSF cung cấp khả năng tạo bit ngẫu nhiên cần thiết cho hoạt động mã hóa TOE

Quản lý: FCS\_RBG.1

Không có hoạt động quản lý dự kiến.

Kiểm tra: FCS\_RBG.1

Không có sự kiện có thể kiểm tra nào dự kiến.

1.1.1. FCS\_RBG.1 Tạo bit ngẫu nhiên

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| FCS\_RBG.1.1 | TSF sẽ tạo bit ngẫu nhiên bằng cách sử dụng bộ tạo bit ngẫu nhiên được lựa chọn đáp ứng sau đây [lựa chọn: *danh sách các tiêu chuẩn*]. |

2. Bảo vệ dữ liệu người dùng

2.1. Toàn vẹn dữ liệu được lưu trữ bên ngoài

Họ hành vi

Họ này xác định các yêu cầu xử lý tính toàn vẹn dữ liệu người dùng được lưu trữ trong các thùng chứa không được kiểm soát bởi TSF.

Cân bằng các thành phần

1

FDP\_EDI : Toàn vẹn dữ liệu được lưu trữ bên ngoài

FDP\_EDI.1 Hành động phản hồi và xác minh tính toàn vẹn của dữ liệu được lưu trữ bên ngoài yêu cầu xác minh dữ liệu được lưu trữ bên ngoài của TSF về lỗi toàn vẹn được xác định và yêu cầu hành động phản hồi cần được thực hiện do phát hiện lỗi.

Quản lý : FDP\_EDI.1

Các hành động sau đây có thể được xem xét cho các chức năng quản lý trong FMT:

a) Lựa chọn dữ liệu người dùng toàn vẹn được lưu trữ bên ngoài để bảo vệ.

b) Có thể tổ chức hành động phản hồi cần thực hiện trong trường hợp phát hiện lỗi toàn vẹn.

Kiểm tra : FDP\_EDI.1

1. Tối thiểu : Kết quả xác minh tính toàn vẹn (thành công, thất bại) và hành động phản hồi

2.1.1. FDP\_EDI.1 Hành động phản hồi và xác minh tính toàn vẹn của dữ liệu được lưu trữ bên ngoài

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc: | Không có thành phần nào khác. |
| FDP\_EDI.1.1 | TSF sẽ xác minh tính toàn vẹn của [lựa chọn: *danh sách có thể định cấu hình của quản trị viên về dữ liệu người dùng được lưu trữ bên ngoài*]. |
| FDP\_EDI.1.2 | Khi phát hiện lỗi toàn vẹn dữ liệu người dùng được lưu trữ bên ngoài, TSF sẽ [lựa chọn: *hành động được thực hiện*] |

|  |
| --- |
| Lưu ý áp dụng   * Trong FDP\_EDI.1.1, [lựa chọn: danh sách dữ liệu người dùng được lưu trữ bên ngoài có thể định cấu hình của quản trị viên] đề cập đến đối tượng dữ liệu người dùng được lưu trữ bên ngoài để xác minh tính toàn vẹn. * Trong FDP\_EDI.1.2, báo động, gửi email, v.v. đến quản trị viên được ủy quyền có thể được nêu trong [lựa chọn : hành động cần thực hiện]. |

3. Quản lý an toàn

3.1. ID and password

Họ hành vi

Họ này xác định các yêu cầu xử lý tính toàn vẹn dữ liệu người dùng được lưu trữ trong các thùng chứa không được kiểm soát bởi TSF.

Cân bằng các thành phần

1

ID và mật khẩu FMT\_PWD

FMT\_PWD.1 Quản lý ID và mật khẩu, yêu cầu TSF cung cấp chức năng quản lý ID và mật khẩu.

Quản lý : FDP\_EDI.1

Kiểm tra: FMT\_PWD.1

Các hành động sau sẽ có thể kiểm tra được nếu FAU\_GEN Tạo dữ liệu kiểm tra bảo mật được bao gồm trong PP/ST:

1. Tối thiểu: Tất cả các thay đổi của mật khẩu

3.1.1. FMT\_PWD.1 Quản lý ID và mật khẩu

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác |
| Các thành phần phụ thuộc | FMT\_SMF.1 Đặc tả chức năng quản lý FMT\_SMR.1 Vai trò bảo mật |
| FMT\_PWD.1.1 | TSF phải hạn chế khả năng quản lý mật khẩu của [lựa chọn: *danh sách các chức năng*] thành [lựa chọn: *các vai trò được xác định có thẩm quyền*].  1. [lựa chọn*: quy tắc kết hợp mật khẩu và/hoặc độ dài*]  2. [lựa chọn: *quản lý khác như quản lý các ký tự đặc biệt không sử dụng được cho mật khẩu, v.v.*] |
| FMT\_PWD.1.2 | TSF phải hạn chế khả năng quản lý ID của [lựa chọn: *danh sách các chức năng*] thành [*lựa chọn: các vai trò được xác định có thẩm quyền*].  1. [lựa chọn: quy tắc kết hợp ID và/hoặc độ dài]  2. [lựa chọn: *quản lý khác như quản lý các ký tự đặc biệt không sử dụng được cho ID, v.v.]* |
| FMT\_PWD.1.3 | TSF sẽ cung cấp khả năng cho [lựa chọn, chọn một trong số: *thiết lập ID và mật khẩu khi cài đặt, thiết lập mật khẩu khi cài đặt, thay đổi ID và mật khẩu khi quản trị viên được ủy quyền truy cập lần đầu tiên, thay đổi mật khẩu khi được ủy quyền quản trị viên truy cập lần đầu tiên].* |

|  |
| --- |
| Lưu ý áp dụng   * Nếu TOE không cung cấp khả năng quản lý quy tắc kết hợp ID và mật khẩu theo vai trò được ủy quyền, v.v., 'Không có' có thể được lựa chọn trong hoạt động gán của FMT\_PWD.1.1, FMT\_PWD.1.2. * Quy tắc kết hợp ID và mật khẩu có thể được đặt bởi vai trò được ủy quyền có thể bao gồm cài đặt độ dài tối thiểu và tối đa, cài đặt quy tắc trộn liên quan đến chữ hoa/chữ thường/số/ký tự đặc biệt của tiếng Anh, v.v.. |

4. Bảo vệ TSF

4.1. Các thực thể bên ngoài có thể liên kết

Họ hành vi

Họ này (FPT\_LEE, Các thực thể bên ngoài có thể liên kết) xác định yêu cầu đối với TSF để thực hiện các chức năng an toàn với sự hỗ trợ của các thực thể bên ngoài. Trong họ này, các thực thể bên ngoài đề cập đến phần mềm hoặc phần cứng, nhưng người dùng không được tính là các thực thể bên ngoài.

Cân bằng các thành phần

1

FMT\_LEE Các thực thể bên ngoài có thể liên kết

FPT\_LEE.1, các thực thể bên ngoài có thể liên kết, yêu cầu TSF cung cấp các chức năng bảo mật bằng cách liên kết với các thực thể bên ngoài.

Quản lý: FMT\_LEE.1

Không dự kiến ​​hoạt động quản lý nào.

Kiểm tra: FPT\_LEE.1

Bạn nên ghi lại các hành động sau để kiểm tra nếu FAU\_GEN Họ tạo dữ liệu kiểm tra bảo mật được bao gồm trong PP/ST:

1. Tối thiểu: Kết quả của việc thực hiện chức năng an toàn được cung cấp bằng cách liên kết với các thực thể bên ngoài

4.1.1. FPT\_LEE.1 Các thực thể bên ngoài có thể liên kết

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| FPT\_LEE.1.1 | TSF sẽ thực hiện [lựa chọn: *danh sách các hành động*] và cung cấp [lựa chọn: *danh sách các chức năng*] liên quan đến các thực thể bên ngoài. |

|  |
| --- |
| Lưu ý áp dụng   * Trong FPT\_LEE.1.1, [lựa chọn: Danh sách hành động] có nghĩa là cách TSF được liên kết với các thực thể bên ngoài, chẳng hạn như lệnh gọi hàm API. * Trong FPT\_LEE.1.1, [lựa chọn: Danh sách các chức năng] sẽ lựa chọn các chức năng an toàn (ví dụ: xác minh bí mật, bảo vệ phản hồi xác thực, v.v.) do TSF cung cấp trong liên kết với các thực thể bên ngoài |

4.4.2. Bảo vệ dữ liệu TSF được lưu trữ

Họ Hành vi

Họ này xác định các quy tắc để bảo vệ dữ liệu TSF được lưu trữ bên trong các cơ sở dữ liệu do TSF kiểm soát khỏi bị sửa đổi hoặc tiết lộ trái phép.

Cân bằng các thành phần

1

FPT\_PST Bảo vệ dữ liệu TSF được lưu trữ

FPT\_PST.1 Bảo vệ cơ bản dữ liệu TSF được lưu trữ, yêu cầu bảo vệ dữ liệu TSF được lưu trữ trong các thùng chứa do TSF kiểm soát.

Quản lý: FPT\_PST.1

Không có hoạt động quản lý dự kiến.

Kiểm toán: FPT\_PST.1

Không có sự kiện nào có thể kiểm toán được dự kiến

4.4.2.1. FPT\_PST.1 Bảo vệ cơ bản dữ liệu TSF được lưu trữ

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc | Không có phụ thuộc. |
| FPT\_PST.1.1 | TSF phải bảo vệ [lựa chọn: *dữ liệu TSF*] được lưu trữ trong các thùng chứa do TSF kiểm soát khỏi [lựa chọn: *tiết lộ, sửa đổi*] trái phép. |

|  |
| --- |
| Lưu ý áp dụng   * Các bộ chứa được điều khiển bởi TSF có nghĩa là lưu trữ trong TOE hoặc các thực thể bên ngoài (DBMS, v.v.) tương tác với TOE. * Ví dụ về dữ liệu TSF cần được bảo vệ như sau:   - Mật khẩu người dùng, khóa mật mã (khóa chia sẻ trước, khóa đối xứng, khóa riêng, v.v.), giá trị cấu hình TOE (chính sách bảo mật, tham số cấu hình), dữ liệu kiểm tra, v.v.   * Các Dữ liệu TSF có thể được mã hóa và lưu trữ để bảo vệ khỏi bị tiết lộ hoặc sửa đổi trái phép |

5. Cập nhật TSF

Họ hành vi

Họ này xác định các yêu cầu cập nhật phần mềm/phần mềm TOE.

Cân bằng các thành phần

1

FPT\_TUD: Cập nhật TSF

Bản cập nhật bản vá bảo mật TSF FPT\_TUD.1, yêu cầu bản cập nhật đáng tin cậy của chương trình cơ sở/phần mềm TOE bao gồm khả năng xác minh tính hợp lệ trên tệp cập nhật trước khi cài đặt bản cập nhật.

Quản lý: FPT\_TUD.1

Các hành động sau có thể được xem xét đối với các chức năng quản lý trong FMT:

1. Quản lý cơ chế xác minh tệp cập nhật

Kiểm tra: FPT\_TUD.1

Các hành động sau có thể kiểm tra được nếu bao gồm FAU\_GEN Tạo dữ liệu kiểm tra bảo mật trong PP/ST:

1. Tối thiểu: Cập nhật kết quả xác minh tệp (thành công, thất bại) Phân cấp: Không có thành phần nào khác. Các thành phần phụ thuộc: Không phụ thuộc.

5.1. Cập nhật bản vá bảo mật FPT\_TUD.1 TSF

|  |  |
| --- | --- |
| Phân cấp | Không có thành phần nào khác. |
| Các thành phần phụ thuộc: | Không phụ thuộc |
| FPT\_TUD.1.1 | TSF sẽ cung cấp khả năng xem các phiên bản TOE cho [lựa chọn: *các vai trò được xác định có thẩm quyền*]. |
| FPT\_TUD.1.2 | TSF sẽ xác minh tính hợp lệ của các tệp cập nhật bằng cách sử dụng [lựa chọn: *so sánh giá trị băm, xác minh chữ ký số*] trước khi cài đặt các bản cập nhật |

|  |
| --- |
| Lưu ý áp dụng   * TSF sẽ cung cấp khả năng kiểm tra phiên bản hiện tại của TOE được cài đặt và thực thi gần đây nhất bởi các vai trò được ủy quyền. * Các bản cập nhật và bản vá bảo mật mới nhất là rất cần thiết để loại bỏ các lỗ hổng bảo mật. Việc xác minh tính hợp lệ trên các tệp cập nhật là bắt buộc vì việc cài đặt các tệp cập nhật mà không có bất kỳ xác minh nào có thể dẫn đến trục trặc hệ thống hoặc lỗi dịch vụ, v.v. |

Tài liệu tham khảo

[1]. Korean National Protection Profile Web Application Firewall v3.0

[2]. TCVN 8709-1:2011 (ISO/IEC 15408-1:2009) Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn CNTT – Phần 1: Giới thiệu và mô hình tổng quát [CC1].

[3]. TCVN 8709-2:2011 (ISO/IEC 15408-2:2009) Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn CNTT – Phần 2: Các thành phần chức năng an toàn [CC2].

[4]. TCVN 8709-3:2011 (ISO/IEC 15408-:2009) Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn CNTT – Phần 3: Các thành phần đảm bảo an toàn [CC3].

[5]. Tiêu chí chung để đánh giá an toàn CNTT, Phương pháp đánh giá, CCMB-2012-09-004, Phiên bản 3.1, Sửa đổi 4, 9/ 2012 [CEM].

[6]. Các hoạt động đánh giá đối với tường lửa STF cPP, Phiên bản 1.0, 27/2/2015 [SD-FW].

[7]. Các hoạt động đánh giá đối với thiết bị mạng cPP, Phiên bản 1.0, 27/2/2015 [SD-ND].