TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 12819:2020

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – HỒ SƠ BẢO VỆ CHO THIẾT BỊ TƯỜNG LỬA LỌC LƯU LƯỢNG CÓ TRẠNG THÁI

Information technology - Security techniques –

Protection profile for stateful traffic filter firewalls

HÀ NỘI - 2020

Mục lục

Lời nói đầu

TCVN 12819:2020 được xây dựng dựa trên cơ sở tham khảo "collaborative Protection Profile for Stateful Traffic Filter Firewalls" được phát triển bởi Cộng đồng kỹ thuật mạng quốc tế và được phê chuẩn bởi CCRA, phiên bản 1.0, ngày 27/02/2015.

TCVN 12819:2020 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 thiết bị tường lửa lọc lưu lượng có trạng thái

Information Technology - Security techniques - Protection profile for Stateful Traffic Filter Firewalls

1 Phạm vi áp dụng

Tiêu chuẩn này quy định hồ sơ bảo vệ cho thiết bị tường lửa lọc lưu lượng có trạng thái, thể hiện các yêu cầu chức năng an toàn (SFR) và yêu cầu đảm bảo an toàn (SAR) đối với thiết bị tường lửa lọc lưu lượng có trạng thái. Các hoạt động đánh giá cụ thể mà tổ chức đánh giá thực hiện nhằm xác định xem một sản phẩm có đáp ứng hay không các SFR nêu trong tiêu chuẩn này được mô tả trong [SD-ND] và [SD-FW].

Tiêu chuẩn này áp dụng vào quá trình đánh giá an toàn thông tin đối với thiết bị tường lửa lọc lưu lượng có trạng thái 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).

2 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].

Evaluation Activities for Stateful Traffic Filter Firewalls cPP *(Các hoạt động đánh giá đối với hồ sơ bảo vệ cho tường lửa lọc lưu lượng có trạng thái)*, Phiên bản 1.0, 27/2/2015 [SD-FW].

Evaluation Activities for Network Device cPP *(Các hoạt động đánh giá đối với hồ sơ bảo vệ cho thiết bị mạng)*, Phiên bản 1.0, 27/2/2015 [SD-ND].

3 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:

3.1

Quản trị viên (administrator)

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

3.2

Bảo đảm (assurance)

Cơ sở để tin cậy rằng một TOE thỏa mãn các SFR [xem TCVN 8709-1:2011].

3.3

Chuỗi khóa (key chaining)

Phương pháp sử dụng nhiều lớp khóa mã hóa để bảo vệ dữ liệu. Khóa lớp trên mã hóa khóa lớp dưới, khóa lớp dưới mã hóa dữ liệu; số lượng các lớp khóa là bất kỳ.

3.4

Quản trị viên an toàn (security administrator)

Khái niệm quản trị viên an toàn và quản trị viên được sử dụng theo cách có thể hoán đổi nhau trong tiêu chuẩn này.

3.5

Đích đánh giá (Target of Evaluation - TOE)

Một tập phần mềm, phần sụn và/hoặc phần cứng cùng với tài liệu hướng dẫn nếu có [xem TCVN 8709-1:2011].

3.6

Chức năng an toàn của TOE (TOE Security Functionality - TSF)

Tính năng kết hợp tất cả phần cứng, phần mềm, và phần sụn của TOE mà dựa vào đó TOE mới thực thi được chính xác các SFR [xem TCVN 8709-1:2011].

3.7

Dữ liệu chức năng an toàn của TOE (TSF data)

Dữ liệu cho hoạt động của TSF làm cơ sở cho thực thi các yêu cầu.

4 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
OCSP	Giao thức kiểm tra trạng thái chứng thư trực tuyến	Online Certificate Status Protocol
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
XTS	Mật mã khối có thể tinh chỉnh	XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing

5 Giới thiệu Hồ sơ bảo vệ

5.1 Tổng quan về TOE

Tiêu chuẩn này nêu rõ các yêu cầu để đánh giá các tường lửa lọc lưu lượng có trạng thái (sau đây gọi tắt là tường lửa). Các sản phẩm này là các thiết bị bảo vệ ranh giới như các tường lửa chuyên dụng, các bộ định tuyến, các thiết bị chuyển mạch được thiết kế để kiểm soát luồng thông tin giữa các mạng kết nối. Trong một số trường hợp, các tường lửa thực hiện các tính năng an toàn có chức năng tách biệt hai mạng riêng biệt - một mạng đáng tin cậy hoặc được bảo vệ và một mạng nội bộ hoặc bên ngoài không tin cậy như Internet - đó chỉ là một trong nhiều ứng dụng có thể có. Thường thì tường lửa có nhiều kết nối mạng vật lý khả dụng cho nhiều cấu hình cũng như các chính sách về luồng thông tin mạng.

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

5.2 Các trường hợp sử dụng TOE

Tiêu chuẩn này đề cập tới tường lửa thực hiện lọc lưu lượng ở tầng mạng 3 và 4. Một tường lửa là một thiết bị bao gồm phần cứng và phần mềm được kết nối với hai hoặc nhiều mạng riêng biệt và có vai trò là cơ sở hạ tầng trong tổng thể mạng doanh nghiệp.

Lọc lưu lượng có trạng thái có ý tưởng là tường lửa sẽ theo dõi trạng thái của từng kết nối thông qua nó và có khả năng chặn các gói dữ liệu không thuộc về một luồng thông tin hợp lệ. Thông tin như số thứ tự TCP, các ACK, các tùy chọn IP cũng được lưu lại bằng cách lưu trữ các số liệu vào bảng trạng thái động. Các cân nhắc khác trong việc đưa ra quyết định chấp nhận, chặn, hoặc ghi nhật ký các gói tin là dựa vào các cổng và địa chỉ IP nguồn và đích hoặc khi các địa chỉ nguồn hoặc đích không phù hợp với các giao diện được định cấu hình.

Các phiên bản sau của tiêu chuẩn này sẽ được đưa vào chức năng tùy chọn (ví dụ: chế độ trong suốt). Các hồ sơ bảo vệ tường lửa tương lai sẽ được sử dụng để chỉ định các bộ chức năng bổ sung (ví dụ:

lọc ứng dụng). Trong tiêu chuẩn này, các tính năng bổ sung như vậy được bỏ qua nhằm phục vụ cho mục đích đánh giá trừ khi chúng có thể có một số ảnh hưởng về các yêu cầu an toàn được nêu ở đây. Trong khi có nhiều thiết bị sẽ được đánh giá theo tiêu chuẩn này có khả năng thực hiện NAT hoặc PAT, sẽ không có yêu cầu nào quy định về khả năng này.

6 Các tuyên bố tuân thủ

Như đã nêu trong tài liệu viện dẫn, tiêu chuẩn này:

- tuân thủ với TCVN 8709-1:2011; TCVN 8709-2:2011 và TCVN 8709-3:2011;

- là mở rộng Phần 2 (TCVN 8709-2:2011) và tuân thủ Phần 3 (TCVN 8709-3:2011);

- không tuyên bố tuân thủ với hồ sơ bảo vệ nào khác.

Phương pháp áp dụng để đánh giá hồ sơ bảo vệ được nêu trong [CEM]. Hồ sơ bảo vệ này đáp ứng các họ bảo đảm sau đây: APE_CCL.1, APE_ECD.1, APE_INT.1, APE_OBJ.1, APE_REQ.1 và APE_SPD.1.

Để phù hợp với tiêu chuẩn này, một TOE phải chứng minh sự tuân thủ chính xác. Sự tuân thủ chính xác, như là một tập con của sự tuân thủ nghiêm ngặt được nêu trong TCVN 8709, được định nghĩa là ST chứa tất cả các yêu cầu trong điều 9 (đây là những yêu cầu bắt buộc) của tiêu chuẩn này và các yêu cầu có thể có từ Phụ lục A (đây là những SFR tùy chọn) hoặc Phụ lục B (đây là các SFR dựa trên lựa chọn, một số sẽ là bắt buộc theo các lựa chọn được đưa ra trong các SFR khác) của tiêu chuẩn này. Trong khi phép lặp được cho phép, không có yêu cầu bổ sung nào (theo TCVN 8709-2:2011 hoặc 8709-3:2011, hoặc định nghĩa về các thành phần được mở rộng chưa có trong tiêu chuẩn này) được phép đưa vào ST. Hơn nữa, không có yêu cầu nào trong điều 9 của tiêu chuẩn này được phép bỏ qua.

7 Mô tả các vấn đề an toàn

Một tường lửa lọc lưu lượng có trạng thái (được xác định là một thiết bị lọc lưu lượng mạng các tầng 3 và 4 (IP và TCP/UDP) được tối ưu hóa thông qua kiểm tra gói tin có trạng thái) được sử dụng nhằm mục đích cung cấp một bộ các yêu cầu tối thiểu, cơ bản nhằm giảm thiểu các mối đe dọa đã được xác định và mô tả rõ ràng.

Tường lửa có khả năng đối sánh các gói tin tới một kết nối đã kích hoạt (và được phép) đã biết và cho phép các gói tin này, chặn các gói tin khác. Tường lửa thường có chức năng như là một thiết bị ranh giới giữa hai miền an toàn mạng riêng biệt, và do đó, phải cung cấp một bộ chức năng an toàn thông thường tối thiểu. Các yêu cầu chức năng này xác định rõ các giao tiếp được ủy quyền với tường lửa, các khả năng kiểm toán, các truy cập người dùng, các quá trình cập nhật, và các thủ tục tự kiểm tra cho các thành phần quan trọng.

7.1 Các mối đe dọa

Các mối đe dọa đối với tường lửa được phân nhóm theo các lĩnh vực chức năng của thiết bị trong các điều dưới đây.

7.1.1 Các giao tiếp với tường lửa

Một tường lửa kết nối với các thiết bị mạng và các thực thể mạng khác. Các điểm cuối của kết nối này có thể cách xa về mặt địa lý và logic và có thể đi qua một loạt các hệ thống khác. Các hệ thống trung gian có thể không đáng tin cậy tạo ra các cơ hội giao tiếp trái phép với tường lửa hoặc gây hại đến các giao tiếp được ủy quyền. Chức năng an toàn của tường lửa phải có khả năng bảo vệ bất kỳ lưu lượng mạng quan trọng nào (lưu lượng truy cập quản trị, lưu lượng xác thực, lưu lượng kiểm toán...). Việc giao tiếp với tường lửa chia thành hai loại: giao tiếp được ủy quyền và trái phép.

Giao tiếp được ủy quyền bao gồm lưu lượng mạng bình thường được cho phép theo chính sách được khởi nguồn và kết thúc từ tường lửa theo vốn dĩ của mục đích thiết kế. Điều này bao gồm lưu lượng mạng quan trọng, chẳng hạn như quản trị tường lửa và giao tiếp với một máy chủ xác thực hoặc đăng nhập kiểm toán, mà đòi hỏi một kênh an toàn để bảo vệ giao tiếp. Chức năng an toàn của tường lửa bao gồm khả năng đảm bảo chỉ cho phép các giao tiếp được ủy quyền và khả năng cung cấp một kênh an toàn cho lưu lượng mạng quan trọng. Bất kỳ giao tiếp khác với những điều trên được xem là giao tiếp trái phép.

Các mối đe dọa chính đối với các giao tiếp tường lửa được đề cập trong tiêu chuẩn này tập trung vào một thực thể bên ngoài, trái phép có truy cập, sửa đổi hoặc tiết lộ lưu lượng mạng quan trọng. Việc sự lựa chọn các thuật toán mã hóa kém hoặc sử dụng các giao thức đường hầm không chuẩn hóa cũng như các ủy quyền quản trị yếu, chẳng hạn như dùng mật khẩu dễ đoán hoặc sử dụng mật khẩu mặc định, sẽ cho phép một tác nhân đe dọa truy cập trái phép vào tường lửa. Mã hóa yếu hay không có mã hóa hầu như không có hoặc có rất ít sự bảo vệ lưu lượng truy cập, cho phép tác nhân đe dọa đọc, thao tác và/hoặc kiểm soát các dữ liệu quan trọng một cách dễ dàng. Các giao thức đường hầm không chuẩn hóa không chỉ giới hạn khả năng tương tác của tường lửa mà còn thiếu sự đảm bảo và tiêu chuẩn hóa tin cậy.

7.1.1.1 T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Các tác nhân đe dọa có thể cố gắng lấy được quyền truy cập của quản trị viên để vào tường lửa bằng các cách thức bất chính như: giả mạo quản trị viên của tường lửa, giả dạng tường lửa đối với quản trị viên, phát lại phiên quản trị (toàn bộ hoặc các phần được chọn), hoặc thực hiện các cuộc tấn công trung gian, sẽ có được truy cập vào phiên quản trị, hoặc các phiên giữa tường lửa và một thiết bị mạng. Lấy được thành công quyền truy cập quản trị sẽ cho phép các hành động độc hại xâm hại đến các chức năng bảo mật của tường lửa và mạng mà nó cư trú.

7.1.1.2 T.WEAK_CRYPTOGRAPHY

Các tác nhân đe dọa có thể khai thác các thuật toán mã hóa yếu hoặc thực hiện tấn công vét cạn đối với không gian khóa. Các thuật toán mã hóa, chế độ và kích thước khóa được chọn kém sẽ cho phép

kẻ tấn công phá được thuật toán hoặc tấn công vét cạn không gian khóa và cho phép chúng truy cập trái phép, đọc, thao tác và/hoặc kiểm soát lưu lượng với nỗ lực tối thiểu.

7.1.1.3 T.UNTRUSTED_COMMUNICATION_CHANNELS

Các tác nhân đe dọa có thể cố gắng nhắm mục tiêu vào các tường lửa không sử dụng các giao thức đường hầm an toàn được tiêu chuẩn hóa để bảo vệ lưu lượng mạng quan trọng. Kẻ tấn công có thể lợi dụng các giao thức được thiết kế kém hoặc quản lý khóa kém để thực hiện thành công các cuộc tấn công trung gian, phát lại các cuộc tấn công... Các cuộc tấn công thành công sẽ dẫn đến mất tính bảo mật và tính toàn vẹn của lưu lượng mạng quan trọng và có khả năng dẫn đến hư hại của chính tường lửa.

7.1.1.4 T.WEAK_AUTHENTICATION_ENDPOINTS

Các tác nhân đe dọa có thể lợi dụng các giao thức bảo mật sử dụng các phương thức yếu để xác thực các điểm cuối - ví dụ: mật khẩu được chia sẻ có thể đoán được hoặc được truyền tải dưới dạng bản rõ. Hậu quả cũng giống như một giao thức được thiết kế kém, kẻ tấn công có thể giả trang thành quản trị viên hoặc thiết bị khác và kẻ tấn công có thể tự chèn vào luồng mạng và thực hiện một cuộc tấn công trung gian. Kết quả là lưu lượng truy cập mạng quan trọng bị lộ và có thể mất tính bảo mật và tính toàn vẹn và có khả năng tường lửa có thể bị xâm phạm.

7.1.2 Các cập nhật hợp lệ

Cập nhật phần mềm và phần sụn tường lửa là rất cần thiết để đảm bảo duy trì chức năng an toàn của tường lửa. Nguồn và nội dung của bản cập nhật được áp dụng phải được xác nhận bằng các phương pháp mật mã; nếu không, một nguồn không hợp lệ có thể viết các cập nhật phần mềm hoặc phần sụn của chính nó làm phá vỡ chức năng an toàn của tường lửa. Các phương pháp xác nhận nguồn và nội dung của một bản cập nhật phần mềm hoặc phần sụn bằng phương pháp mật mã thường liên quan đến các lược đồ chữ ký mật mã trong đó các giá trị băm của các bản cập nhật được ký số.

Các phiên bản phần mềm hoặc phần sụn chưa được vá sẽ dễ khiến tường lửa dễ bị ảnh hưởng bởi các tác nhân đe dọa đang cố phá vỡ chức năng an toàn bằng cách sử dụng các lỗ hổng đã được biết đến. Các bản cập nhật không được xác nhận hoặc được xác nhận bằng cách sử dụng mật mã hóa không an toàn hoặc yếu sẽ khiến phần mềm hoặc phần sụn được cập nhật dễ bị ảnh hưởng bởi các tác nhân nguy hiểm đang cố sửa đổi phần mềm hoặc phần sụn cho lợi thế của họ.

7.1.2.1 T.UPDATE_COMPROMISE

Các tác nhân đe dọa có thể cố gắng cung cấp bản cập nhật bị xâm phạm của phần mềm hoặc chương trình cơ sở làm suy yếu chức năng bảo mật của thiết bị. Các bản cập nhật không được xác nhận hoặc được xác nhận bằng cách sử dụng mật mã không an toàn hoặc yếu khiến phần mềm cập nhật dễ bị thay đổi lén lút.

7.1.3 Hoạt động kiểm toán

Kiểm toán các hoạt động tường lửa là một công cụ có giá trị để các quản trị viên theo dõi tình trạng của thiết bị. Nó cung cấp phương tiện cho giải trình của quản trị viên, báo cáo hoạt động chức năng an toàn, tái thiết các sự kiện và phân tích vấn đề. Quá trình xử lý để đáp ứng các hoạt động của thiết bị có thể đưa ra các chỉ báo về sự thất bại hoặc hư hại của chức năng an toàn. Khi các chỉ báo về hoạt động có tác động đến chức năng an toàn không được tạo ra và không được giám sát thì có thể các hoạt động như vậy sẽ xảy ra mà quản trị viên không nhận thức được. Hơn nữa, nếu hồ sơ không được tạo lập hoặc giữ lại, thì việc tái thiết mạng và khả năng hiểu được phạm vi của tác động sẽ bị ảnh hưởng tiêu cực. Các mối quan tâm khác là bảo vệ dữ liệu kiểm toán đã được lập hồ sơ khỏi những thay đổi hoặc xóa bỏ trái phép. Điều này có thể xảy ra trong nội bộ TOE, hoặc trong khi dữ liệu kiểm toán đang được chuyển sang thiết bị lưu trữ bên ngoài.

Lưu ý rằng tiêu chuẩn này yêu cầu tường lửa tạo ra dữ liệu kiểm toán và có khả năng gửi dữ liệu kiểm toán đến một thực thể mạng đáng tin cậy (ví dụ: máy chủ *syslog*).

7.1.3.1 T.UNDETECTED_ACTIVITY

Các tác nhân đe dọa có thể cố gắng truy cập, thay đổi, và/hoặc sửa đổi các chức năng bảo mật của tường lửa mà quản trị viên không nhận thức được điều này. Điều này có thể dẫn đến kẻ tấn công tìm ra con đường (ví dụ: cấu hình sai, thiếu sót trong sản phẩm) để xâm nhập thiết bị và quản trị viên sẽ không biết được rằng thiết bị đã bị xâm nhập.

7.1.4 Các ủy nhiệm xác thực quản trị viên, tường lửa và dữ liệu

Tường lửa chứa dữ liệu và các ủy nhiệm xác thực mà các dữ liệu này phải được lưu trữ an toàn và phải hạn chế một cách hợp lý quyền truy cập dành cho các thực thể được ủy quyền. Ví dụ bao gồm cấu hình, phần sụn, phần mềm tường lửa, ủy nhiệm xác thực cho các kênh an toàn và ủy nhiệm xác thực của quản trị viên. Các khóa tường lửa và quản trị viên, các tài liệu quan trọng và ủy nhiệm xác thực cần được bảo vệ khỏi bị tiết lộ trái phép và sửa đổi. Hơn nữa, chức năng an toàn của tường lửa cần yêu cầu thay đổi các ủy quyền xác thực mặc định, chẳng hạn như mật khẩu quản trị viên.

Việc thiếu khả năng lưu trữ an toàn và xử lý không đúng các ủy nhiệm và dữ liệu, chẳng hạn như các ủy nhiệm không được mã hóa bên trong các tệp tin cấu hình hoặc truy cập vào các khóa phiên kênh an toàn, có thể cho phép kẻ tấn công không chỉ truy cập vào tường lửa mà còn làm ảnh hưởng tới tính an toàn của mạng lưới thông qua các sửa đổi được ủy quyền cho cấu hình hoặc các cuộc tấn công trung gian. Các cuộc tấn công này cho phép một thực thể trái phép truy cập và thực hiện các chức năng quản trị bằng các ủy nhiệm của quản trị viên được ủy quyền và ngăn chặn tất cả các lưu lượng như là một điểm cuối được ủy quyền. Điều này dẫn đến khó khăn trong việc phát hiện các tác động có hại tới tính an toàn và tái thiết mạng, có khả năng cho phép truy cập trái phép vào dữ liệu của quản trị viên và tường lửa.

7.1.4.1 T.SECURITY_FUNCTIONALITY_COMPROMISE

Các tác nhân đe dọa có thể tác động các dữ liệu tường lửa và ủy nhiệm và cho phép tiếp tục truy cập vào tường lửa và dữ liệu quan trọng của nó. Các tác động đến ủy nhiệm bao gồm thay thế các ủy nhiệm hiện có bằng ủy nhiệm của kẻ tấn công, sửa đổi các ủy nhiệm hiện có hoặc có được các ủy nhiệm quan trọng của quản trị viên hoặc tường lửa để sử dụng.

7.1.4.2 T.PASSWORD_CRACKING

Các tác nhân đe dọa có thể tận dụng các mật khẩu quản trị yếu để truy cập đặc quyền vào tường lửa. Có quyền truy cập đặc quyền vào tường lửa sẽ giúp cho kẻ tấn công truy cập thoải mái vào lưu lượng mạng mà không bị khóa và có thể cho phép họ tận dụng các mối quan hệ tin cậy từ các thiết bị mạng khác.

7.1.5 Sự thất bại của các thành phần tường lửa

Cơ chế an toàn của tường lửa thường được xây dựng từ các gốc tin cậy tới các bộ cơ chế phức tạp hơn. Các thất bại có thể gây ra các tác động đến các chức năng an toàn của tường lửa. Một tường lửa tự kiểm tra các thành phần quan trọng về an toàn của nó ở cả khi khởi động và trong thời gian chạy sẽ đảm bảo độ tin cậy của chức năng an toàn của tường lửa.

7.1.5.1 T.SECURITY_FUNCTIONALITY_FAILURE

Một thành phần của tường lửa có thể thất bại trong quá trình khởi động hoặc trong quá trình hoạt động gây ra tác động hoặc thất bại trong chức năng an toàn của tường lửa, làm cho tường lửa dễ bị tấn công.

7.1.6 Tiết lộ thông tin trái phép

Các thiết bị trong một mạng được bảo vệ có thể chịu các mối đe dọa gây bởi thiết bị nằm ngoài mạng lưới bảo vệ, đang cố gắng thực hiện các hoạt động trái phép. Nếu các thiết bị bên ngoài độc hại đã biết có thể giao tiếp với các thiết bị trong mạng được bảo vệ hoặc nếu thiết bị trong mạng được bảo vệ có thể thiết lập giao tiếp với các thiết bị bên ngoài này thì những thiết bị bên trong này có thể dễ bị tiết lộ thông tin một cách trái phép.

Từ góc độ xâm nhập vào, các tường lửa có chức năng hạn chế quyền truy cập vào các địa chỉ mạng đích cụ thể và các cổng trong một mạng được bảo vệ. Với những hạn chế này, quá trình quét cổng mạng chung sẽ bị ngăn chặn không để tiếp cận tới các mạng hay các máy được bảo vệ cũng như việc truy cập thông tin trên mạng được bảo vệ có thể bị giới hạn ở các cổng được định cấu hình cụ thể trên các nút mạng đã được xác định (ví dụ các trang web từ một máy chủ web của công ty được chỉ định). Ngoài ra, truy cập có thể được giới hạn ở chỉ các địa chỉ và cổng nguồn cụ thể để các mạng hoặc nút mạng cụ thể có thể bị chặn truy cập vào mạng được bảo vệ do đó hạn chế hơn nữa khả năng tiết lộ thông tin.

Từ góc độ rò rỉ ra ngoài, các tường lửa có chức năng hạn chế làm thế nào các nút mạng hoạt động trên một mạng được bảo vệ có thể kết nối và giao tiếp với các mạng khác giới hạn cách thức và địa

điểm phổ biến thông tin. Các mạng bên ngoài cụ thể có thể bị chặn hoàn toàn hoặc các đường đi ra có thể bị giới hạn ở các địa chỉ và/hoặc cổng cụ thể. Ngoài ra, các tùy chọn đi ra sẵn có cho các nút mạng trên mạng được bảo vệ có thể được bảo vệ để đảm bảo rằng các kết nối ra ngoài được định tuyến qua các proxy hoặc bộ lọc ủy quyền để giảm thiểu việc tiết lộ không thích hợp của dữ liệu được đẩy ra.

7.1.6.1 T.NETWORK_DISCLOSURE

Một kẻ tấn công có thể cố gắng "ánh xạ" một mạng con để xác định các máy nằm trên mạng, và lấy cấp địa chỉ IP của các máy, cũng như các dịch vụ (các cổng) mà các máy đó đang cung cấp. Thông tin này có thể được sử dụng để gắn các cuộc tấn công vào các máy đó thông qua các dịch vụ được xuất ra.

7.1.7 Tiếp cận không phù hợp tới các dịch vụ

Các thiết bị nằm bên ngoài mạng được bảo vệ có thể tìm cách thực hiện các dịch vụ nằm trên mạng được bảo vệ mà chỉ dành cho truy cập từ bên trong mạng được bảo vệ. Các thiết bị nằm ngoài mạng được bảo vệ cũng có thể cung cấp các dịch vụ không phù hợp cho truy cập từ bên trong mạng được bảo vệ.

Từ góc độ ngoài vào, tường lửa có thể được cấu hình để chỉ có những máy chủ mạng được thiết kế dành cho truy cập từ bên ngoài có thể truy cập được và chỉ thông qua các cổng chỉ định. Điều này giúp giảm thiểu khả năng các thực thể mạng bên ngoài một mạng được bảo vệ truy cập các máy chủ mạng hoặc dịch vụ chỉ dành cho sử dụng hoặc truy cập bên trong một mạng được bảo vệ.

Từ góc độ trong ra, các tường lửa có thể được định cấu hình để chỉ những dịch vụ bên ngoài cụ thể (ví dụ, dựa vào cổng đích) có thể được truy cập từ bên trong một mạng được bảo vệ. Ví dụ, việc truy cập vào các dịch vụ thư bên ngoài có thể bị chặn để thực thi các chính sách của công ty đối với việc truy cập các máy chủ email không kiểm soát được. Lưu ý rằng hiệu quả của một tường lửa khá hạn chế đối với vấn đề này vì các máy chủ bên ngoài có thể cung cấp dịch vụ trên các cổng thay thế - đây là nơi tường lửa lọc ứng dụng (Application Filter Firewall) cung cấp bảo vệ đáng tin cậy hơn.

7.1.7.1 T.NETWORK_ACCESS

Với kiến thức về các dịch vụ được xuất ra bởi các máy trên mạng con, kẻ tấn công có thể cố gắng khai thác các dịch vụ đó bằng cách gắn các tấn công vào các dịch vụ đó.

7.1.8 Sử dụng sai dịch vụ

Các thiết bị nằm ngoài một mạng "được bảo vệ", trong khi được phép truy cập các dịch vụ công cộng cụ thể được cung cấp bên trong mạng được bảo vệ, có thể cố thực hiện các hoạt động không phù hợp khi đang giao tiếp với các dịch vụ công cộng được phép. Một số dịch vụ nhất định được cung cấp trong mạng được bảo vệ cũng có thể chứa rủi ro khi truy cập từ bên ngoài mạng được bảo vệ. Cần lưu ý rằng tường lửa chỉ đơn giản thực thi các quy tắc được cụ thể cho một giao diện mạng. Quan niệm về một mạng được bảo vệ hoặc đáng tin cậy là sự đúc rút rất hữu ích khi xây dựng bộ quy tắc.

Từ góc độ xâm nhập vào, người ta thường giả định rằng các thực thể hoạt động trên các mạng bên ngoài không bị ràng buộc bởi các chính sách sử dụng cho một mạng được bảo vệ nhất định. Tuy nhiên, các tường lửa có thể ghi lại hành vi vi phạm chính sách thể hiện sự vi phạm các tuyên bố sử dụng công khai cho các dịch vụ công cộng hiện có.

Từ góc độ rò rỉ ra ngoài, các tường lửa có thể được cấu hình để giúp thực thi và giám sát các chính sách sử dụng mạng được bảo vệ. Như đã giải thích trong các mối đe dọa khác, một tường lửa có thể hạn chế việc phổ biến dữ liệu, truy cập các máy chủ bên ngoài, và thậm chí là gián đoạn dịch vụ - tất cả những điều này có thể liên quan đến các chính sách sử dụng của một mạng được bảo vệ và như vậy là đối tượng của một số quan tâm về thực thi. Ngoài ra, tường lửa có thể được cấu hình để ghi lại các sử dụng mạng giữa mạng được bảo vệ và mạng bên ngoài và do đó có thể có tác dụng xác định các vi phạm chính sách sử dụng có thể có.

7.1.8.1 T.NETWORK_MISUSE

Kẻ tấn công có thể cố sử dụng các dịch vụ được xuất bởi các máy theo cách thức không được chủ ý bởi các chính sách an toàn của một site. Ví dụ, một kẻ tấn công có thể sử dụng một dịch vụ để "ẩn danh" máy của kẻ tấn công khi họ tấn công các máy khác.

7.1.9 Lưu lượng độc hại

Một tường lửa cũng cung cấp bảo vệ chống lại các gói dữ liệu độc hại hoặc bị thay đổi. Nó sẽ bảo vệ chống lại các cuộc tấn công như sửa đổi thông tin trạng thái kết nối và các cuộc tấn công lặp lại. Các cuộc tấn công này có thể khiến tường lửa, hoặc các thiết bị mà nó bảo vệ, cấp quyền truy cập trái phép hoặc thậm chí là tạo lập Từ chối dịch vụ.

7.1.9.1 T.MALICIOUS_TRAFFIC

Kẻ tấn công có thể cố gắng gửi các gói thông tin không đúng định dạng tới một máy tính với hy vọng gây ra tình trạng ngăn xếp mạng hoặc các dịch vụ đang lắng nghe trên các cổng UDP/TCP của máy đích bị sự cố.

7.2 Các giả định

Điều này mô tả các giả định được thực hiện trong việc xác định các mối đe dọa và yêu cầu an toàn đối với tường lửa. Tường lửa không được kỳ vọng cung cấp đảm bảo trong bất kỳ khu vực nào, và do đó, không đưa ra các yêu cầu để giảm thiểu các mối đe dọa liên quan này.

7.2.1 A.PHYSICAL_PROTECTION

Tường lửa được giả định là được bảo vệ về mặt vật lý trong môi trường hoạt động của nó và không bị các cuộc tấn công làm ảnh hưởng đến an toàn và/hoặc can thiệp vào các kết nối vật lý cũng như vận hành chính xác của tường lửa. Bảo vệ này được giả định là đủ để bảo vệ tường lửa và dữ liệu nó chứa. Do đó, PP này sẽ không đưa vào bất kỳ yêu cầu nào về bảo vệ chống trộm cắp hoặc các biện

pháp giảm thiểu tấn công vật lý khác. PP này sẽ không mong đợi sản phẩm bảo vệ ngăn các truy cập vào tường lửa cho phép các thực thể trái phép trích xuất dữ liệu, vượt qua các kiểm soát khác, hoặc thao tác với tường lửa.

[OE.PHYSICAL]

7.2.2 A.LIMITED_FUNCTIONALITY

Tường lửa được giả định là cung cấp chức năng kết nối mạng và lọc làm chức năng cốt lõi và không cung cấp các chức năng/dịch vụ có thể được coi là tính toán mục đích chung. Ví dụ, tường lửa không nên cung cấp nền tảng tính toán cho các ứng dụng mục đích chung (không liên quan đến chức năng kết nối mạng/lọc).

[OE.NO_GENERAL_PURPOSE]

7.2.3 A.TRUSTED_ADMINSTRATOR

Các quản trị viên được ủy quyền cho tường lửa được giả định là đáng tin cậy và hành động vì lợi ích cao nhất về an toàn cho tổ chức. Điều này bao gồm đào tạo phù hợp, tuân thủ chính sách, và bám sát các tài liệu hướng dẫn. Quản trị viên phải đáng tin cậy để đảm bảo mật khẩu/ủy nhiệm đủ mạnh và entropy và không có ý định gây độc hại khi quản trị tường lửa. Tường lửa không kỳ vọng có khả năng chống lại quản trị viên giả mạo thực hiện việc chủ động vượt qua hoặc làm ảnh hưởng đến tính an toàn của nó.

[OE.TRUSTED_ADMIN]

7.2.4 A.REGULAR_UPDATES

Phần mềm và phần sụn tường lửa được giả định được quản trị viên cập nhật thường xuyên các bản cập nhật đã phát hành khi lỗ hổng đã được phát hiện.

[OE.UPDATES]

7.2.5 A.ADMIN_CREDENTIALS_SECURE

Các ủy nhiệm của quản trị viên (khóa riêng) được sử dụng để truy cập vào tường lửa được bảo vệ bởi nền tảng máy chủ lưu trữ.

[OE.ADMIN_CREDENTIALS_SECURE]

7.3 Chính sách an toàn của tổ chức

Chính sách an toàn của tổ chức là một tập hợp các quy tắc, phương pháp và thủ tục do một tổ chức ban hành để đáp ứng nhu cầu an toàn. Để phục vụ cho các mục đích của tiêu chuẩn này, một chính sách duy nhất được mô tả trong các điều dưới đây.

7.3.1 P.ACCESS_BANNER

TOE sẽ hiển thị biểu ngữ ban đầu mô tả các hạn chế sử dụng, các thỏa thuận pháp lý hoặc bất kỳ thông tin thích hợp nào khác mà người dùng sẽ đồng ý khi truy cập vào TOE.

[FTA_TAB.1]

8 Các mục tiêu an toàn

8.1 Các mục tiêu an toàn cho môi trường hoạt động

Các điều dưới đây mô tả các mục tiêu cho môi trường hoạt động.

8.1.1 OE.PHYSICAL

An toàn vật lý, tương xứng với giá trị của TOE và dữ liệu mà nó chứa đựng, được cung cấp bởi môi trường.

8.1.2 OE.NO_GENERAL_PURPOSE

Không có khả năng tính toán mục đích chung (ví dụ, trình biên dịch hoặc các ứng dụng người dùng) có sẵn trên TOE, ngoài các dịch vụ cần thiết cho hoạt động, quản lý và hỗ trợ của TOE.

8.1.3 OE.TRUSTED_ADMIN

Quản trị viên TOE được tin cậy tuân thủ và áp dụng tất cả tài liệu hướng dẫn một cách đáng tin cậy.

8.1.4 OE.UPDATES

Phần sụn và phần mềm TOE được cập nhật thường xuyên bởi một quản trị viên để đáp ứng kịp thời với việc phát hành bản cập nhật sản phẩm do các lỗ hổng được biết đến.

8.1.5 OE.ADMIN_CREDENTIALS_SECURE

Các ủy nhiệm của quản trị viên (khóa bí mật) được sử dụng để truy cập vào TOE phải được bảo vệ trên bất kỳ nền tảng khác mà chúng lưu trú.

9 Các yêu cầu chức năng an toàn

Các yêu cầu chức năng an toàn được quy định trong các điều dưới đây. Các SFR trong điều này là các SFR bắt buộc mà bất kỳ TOE tuân thủ nào phải đáp ứng. Dựa trên các lựa chọn được đưa ra trong các SFR, việc đưa vào một số SFR dựa trên lựa chọn trong Phụ lục B cũng rất cần thiết. Các SFR tùy chọn bổ sung cũng có thể được áp dụng từ những yêu cầu được liệt kê trong Phụ lục A.

Các hoạt động đánh giá được định nghĩa trong [SD] mô tả những hành động nhà đánh giá sẽ thực hiện để xác định sự tuân thủ của một TOE cụ thể với các SFR. Do đó, nội dung của các hoạt động đánh giá này sẽ cung cấp nhiều thông tin chi tiết hơn về các sản phẩm cần thiết được yêu cầu từ các nhà phát triển TOE.

9.1 Các quy ước

Các quy ước được sử dụng để mô tả các SFR như sau:

- Chỉ định: được trình bày dưới dạng văn bản *in nghiêng*;

- Tinh chỉnh bởi tác giả PP: được trình bày **in đậm** và ~~gạch ngang~~, nếu cần;

- Lựa chọn: được trình bày dưới dạng văn bản gạch chân;

- Chỉ định trong một lựa chọn: được trình bày dưới dạng văn bản *in nghiêng và gạch chân*;

- Lặp lại: được thể hiện bằng cách viết thêm số lần lặp trong ngoặc đơn, ví dụ, (1), (2), (3) và/hoặc bằng cách thêm một chuỗi bắt đầu bằng "/".

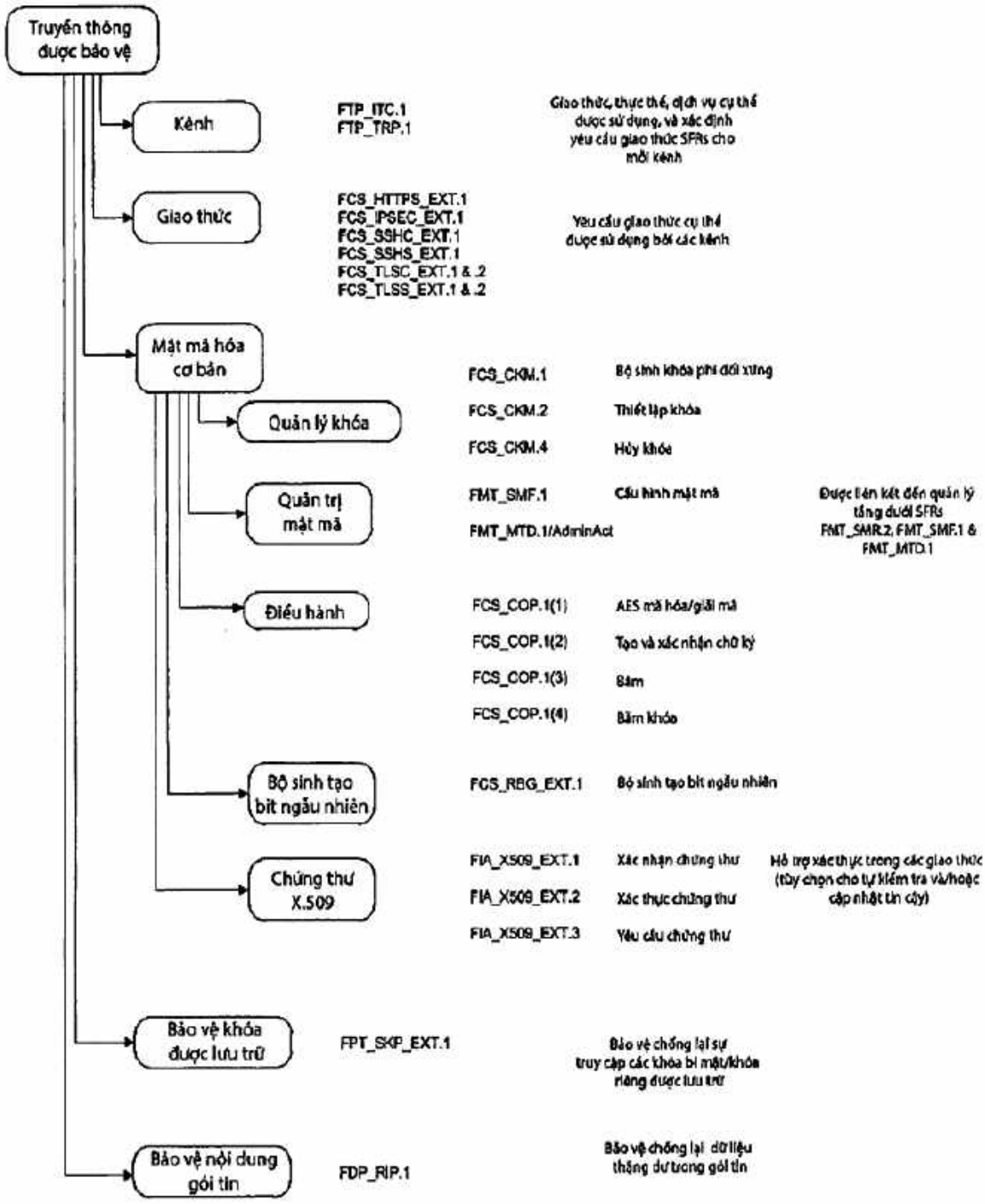
Các SFR mở rộng được xác định bằng cách đặt một nhãn 'EXT' ở cuối tên SFR.

9.2 Cấu trúc SFR

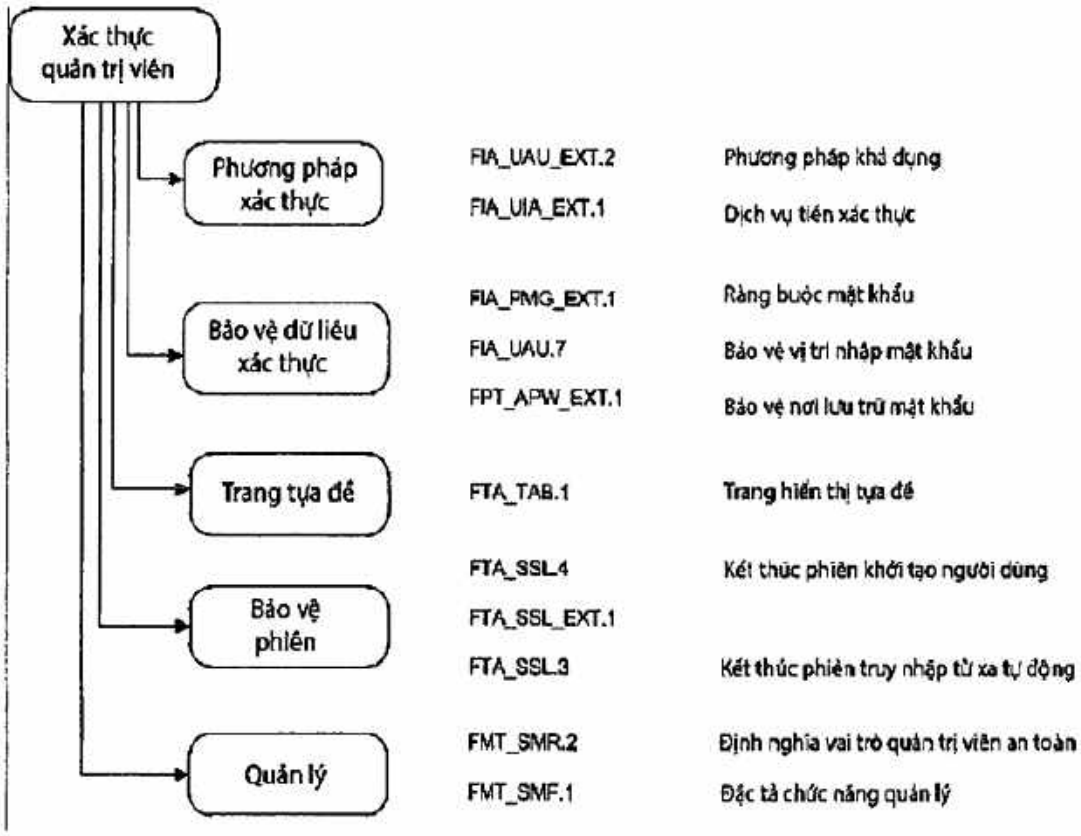
Hình 1, Hình 2, Hình 3, Hình 4, Hình 5 và Hình 6 thể hiện liên kết giữa các yêu cầu chức năng an toàn (SFR) trong điều 9.3 - 9.11, Phụ lục A và Phụ lục B, và các khu chức năng cơ bản cũng như các hoạt động mà TOE cung cấp. Các biểu đồ cung cấp một bối cảnh cho các SFR liên quan đến việc sử dụng chúng trong TOE, trong khi các điều khác xác định các SFR được nhóm bởi lớp trừu tượng và các họ (family) theo quy định TCVN 8709-2:2011.

Nhìn chung, các SFR từ Phụ lục B được yêu cầu bởi ST được xác định bởi các lựa chọn được thực hiện trong các SFR khác. Ví dụ: FTP_ITC.1 và FTP_TRP.1 (trong các điều 9.10.1.1 và 9.10.2.1) mỗi điều đều có các lựa chọn của một giao thức được sử dụng cho loại kênh an toàn được mô tả bởi SFR. Việc lựa chọn (các) giao thức ở đây quyết định các SFR cụ thể theo giao thức nào trong điều B.2.1 cũng được yêu cầu trong ST.

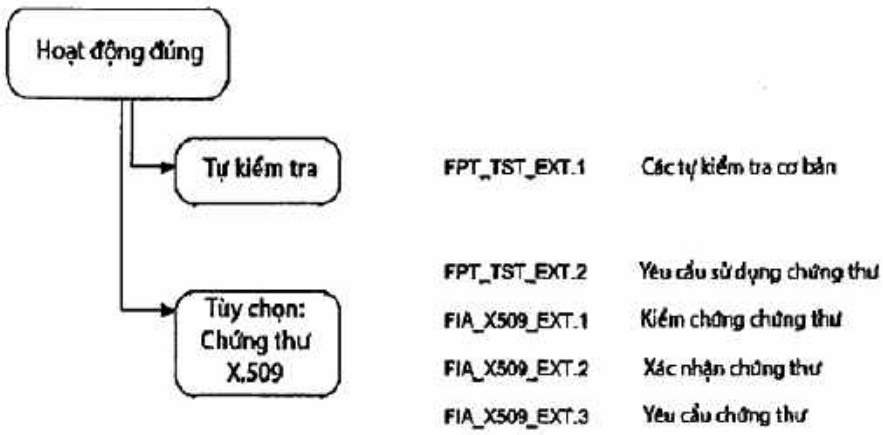
Các SFR trong Phụ lục A có thể được đưa vào ST nếu chúng được cung cấp bởi TOE, nhưng không bắt buộc để TOE xác nhận sự phù hợp với tiêu chuẩn này.



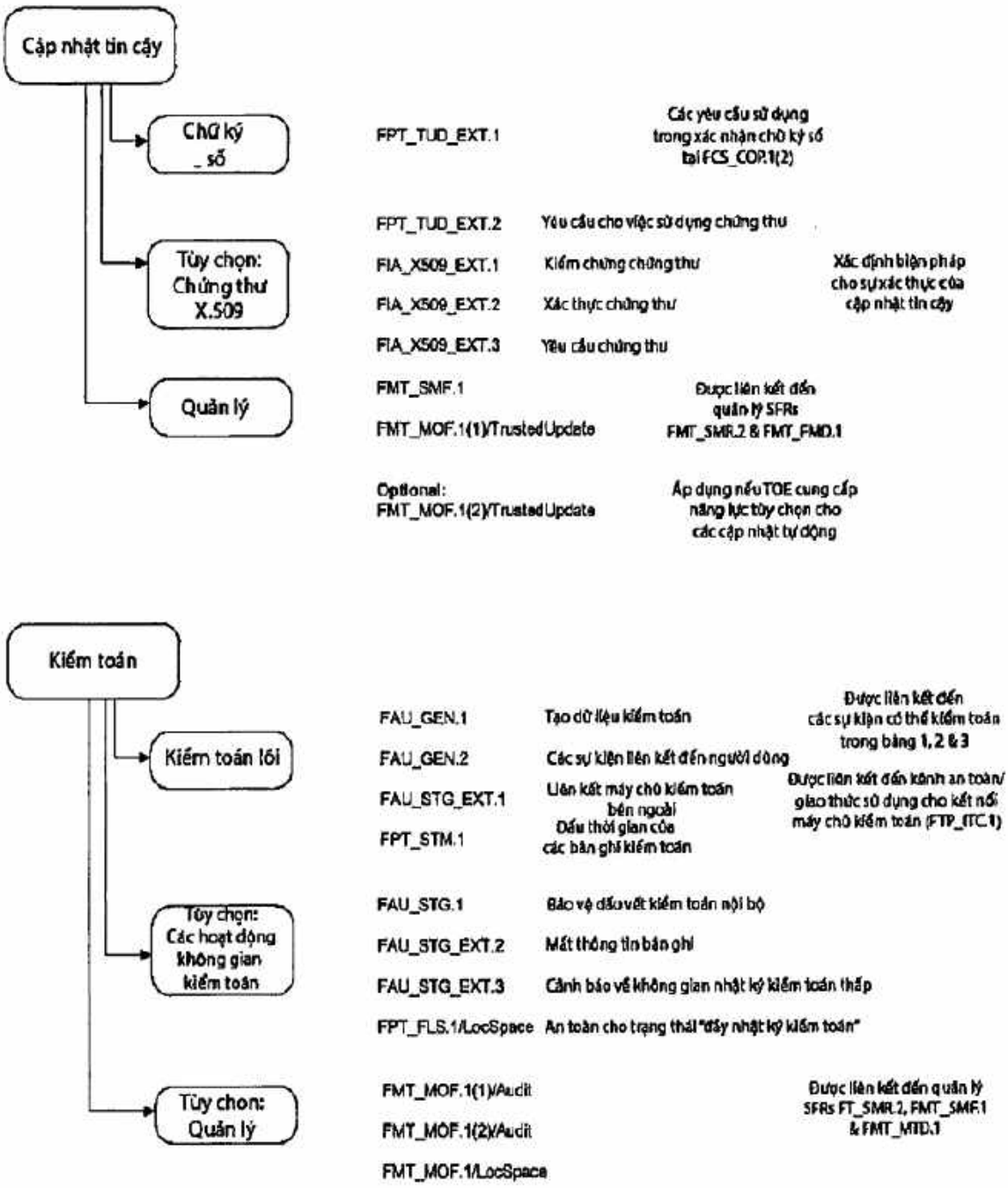
Hình 1 - Cấu trúc SFR trong các truyền thông được bảo vệ



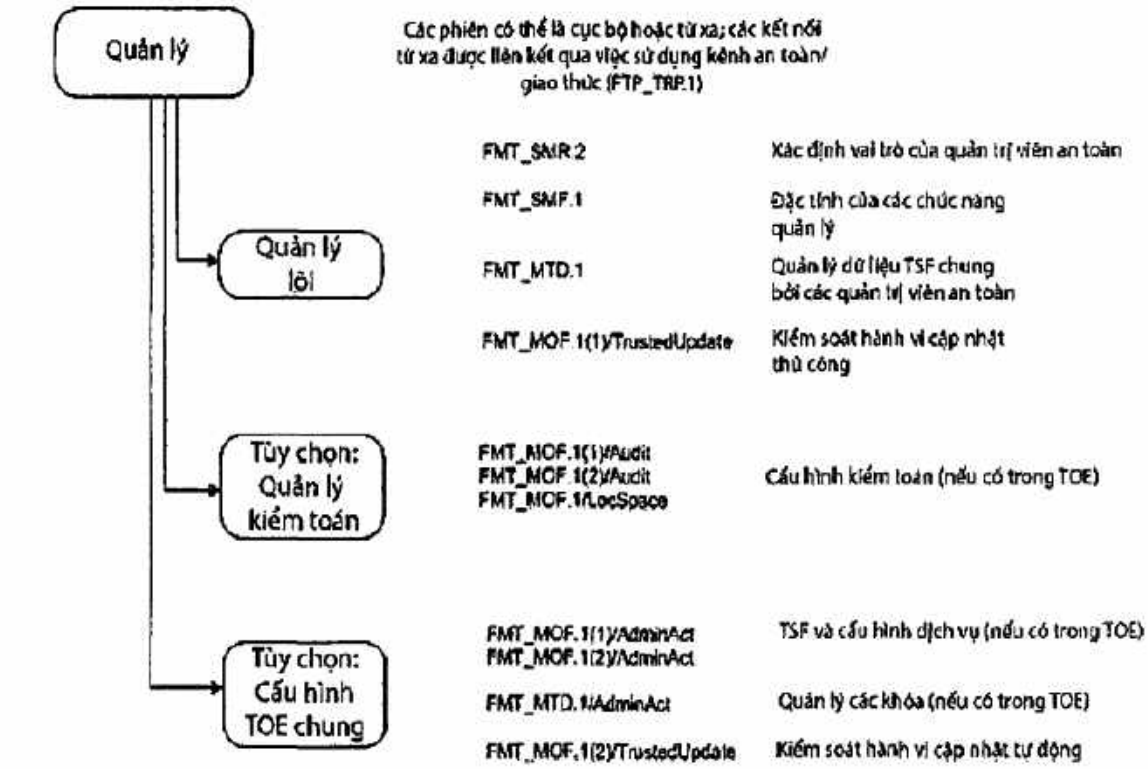
Hình 2 - Cấu trúc SFR trong xác thực quản trị viên



Hình 3 - Cấu trúc SFR trong hoạt động chính xác



Hình 4 - Cấu trúc SFR trong kiểm toán và cập nhật tin cậy



Hình 5 - Cấu trúc SFR trong quản lý

Hình 6 - Cấu trúc SRF trong quy tắc tường lửa

9.3 Kiểm toán an toàn (FAU)

9.3.1 Tạo dữ liệu kiểm toán an toàn (FAU_GEN)

Để đảm bảo rằng thông tin tồn tại cho phép các quản trị viên phát hiện các vấn đề cố ý và không chủ ý với cấu hình và/hoặc hoạt động của hệ thống, thì các TOE tuân thủ phải có khả năng tạo ra các dữ liệu kiểm toán nhằm mục đích phát hiện hoạt động đó. Việc kiểm toán các hoạt động quản trị cung cấp thông tin có thể được sử dụng để thúc đẩy hành động khắc phục nếu hệ thống không được cấu hình chính xác. Kiểm toán các sự kiện hệ thống đã chọn có thể cung cấp dấu hiệu của sự thất bại của các phần quan trọng của TOE (ví dụ như quá trình cung cấp mật mã không hoạt động) hoặc hoạt động bất thường đáng ngờ (ví dụ như thiết lập phiên quản trị vào một thời điểm đáng ngờ, các thất bại lặp lại trong việc thiết lập các phiên hoặc xác thực với hệ thống).

Trong một số trường hợp, có thể có một lượng lớn thông tin kiểm toán được sinh ra có thể áp đảo TOE hoặc các quản trị viên có trách nhiệm xem xét thông tin kiểm toán. TOE phải có khả năng gửi thông tin kiểm toán tới một thực thể tin cậy bên ngoài. Thông tin này phải có dấu thời gian (timestamp) đáng tin cậy, giúp sắp xếp thông tin khi gửi đến thiết bị bên ngoài.

Mất liên lạc với máy chủ kiểm toán là điều nguy hiểm. Mặc dù có nhiều cách để giảm thiểu nguy cơ này, nhưng tiêu chuẩn này không bắt buộc phải có hành động cụ thể; mức độ để hành động này bảo toàn thông tin kiểm toán và vẫn cho phép TOE đáp ứng các chức năng của nó sẽ quyết định về tính phù hợp của TOE trong một môi trường cụ thể.

9.3.1.1 FAU_GEN.1 Tạo dữ liệu kiểm toán

FAU_GEN.1.1 TSF phải tạo ra một hồ sơ kiểm toán cho các sự kiện kiểm toán sau:

a) Khởi động và đóng các chức năng kiểm toán;

b) Tất cả các sự kiện có thể kiểm toán được đối với mức kiểm toán không xác định; và

c) Tất cả các hành động quản trị bao gồm:

- Đăng nhập và đăng xuất (tên của tài khoản người dùng sẽ được đăng nhập nếu tài khoản người dùng cá nhân được yêu cầu cho quản trị viên).

- Thay đổi cấu hình liên quan đến an toàn (bên cạnh thông tin về một thay đổi đã xảy ra, thì những gì đã được thay đổi phải được ghi lại).

- Tạo ra/nhập vào, thay đổi, hoặc xóa các khóa mã hóa (bên cạnh các hành động, một tham chiếu khóa hay tên khóa phải được ghi lại.)

- Thiết lập lại mật khẩu (tên của tài khoản người dùng liên quan phải được ghi lại).

- Khởi động và dừng dịch vụ (nếu áp dụng)

- Lựa chọn: [không các hành động khác, chỉ định: [danh sách sử dụng các đặc quyền khác]];

d) *Các sự kiện có thể kiểm toán được xác định cụ thể được nêu trong Bảng 1.*

Chú thích áp dụng: Nếu danh sách của "các hành động quản trị" xuất hiện không hoàn chỉnh, thì chỉ định trong lựa chọn nên được sử dụng để liệt kê các hành động quản trị bổ sung được kiểm toán.

Tác giả ST thay thế tham chiếu chéo cho các bảng sự kiện kiểm toán với một tham chiếu chéo thích hợp cho ST. Điều này cũng phải bao gồm các phần có liên quan của Bảng 3 và Bảng 4 cho các SFR tùy chọn và các SFR dựa trên lựa chọn có trong ST.

Chú thích áp dụng: Tác giả ST có thể đưa các sự kiện có thể kiểm toán khác một cách trực tiếp vào trong bảng; không giới hạn trong danh sách trình bày.

TSS phải xác định thông tin nào được ghi lại để xác định khóa liên quan cho nhiệm vụ quản trị tạo ra/ nhập vào, thay đổi hoặc xóa các khóa mật mã.

Đối với FAU_GEN.1.1, thuật ngữ "dịch vụ" đề cập đến đường dẫn đáng tin cậy và giao tiếp kênh đáng tin cậy, tự kiểm tra theo yêu cầu, cập nhật tin cậy và các phiên quản trị viên (tồn tại theo đường dẫn đáng tin cậy) (ví dụ netconf).

FAU_GEN.1.2 TSF phải ghi lại trong từng hồ sơ kiểm toán ít nhất thông tin sau:

a) Ngày và giờ của sự kiện, loại sự kiện, chủ đề và kết quả (thành công hay thất bại) của sự kiện; và

b) Đối với từng loại sự kiện kiểm toán, dựa vào các định nghĩa các thành phần chức năng có trong PP/ST, *thông tin ghi trong cột 3 Bảng 1.*

Chú thích áp dụng: Tác giả ST thay thế tham chiếu chéo cho bảng các sự kiện kiểm toán với một tham chiếu chéo thích hợp cho ST. Điều này cũng phải bao gồm các phần có liên quan ở Bảng 3 và Bảng 4 cho các SFR tùy chọn và lựa chọn có trong ST.

Bảng 1 - SFR và các sự kiện có thể kiểm toán

Yêu cầu	Các sự kiện kiểm toán	Nội dung hồ sơ kiểm toán bổ sung
FAU_GEN.1	Không.	Không.
FAU_GEN.2	Không.	Không.
FAU_STG_EXT.1	Không.	Không.
FCS_CKM.1	Không.	Không.
FCS_CKM.2	Không.	Không.
FCS_CKM.4	Không.	Không.
FCS_COP.1(1)	Không.	Không.
FCS_COP.1(2)	Không.	Không.
FCS_COP.1(3)	Không.	Không.
FCS_COP.1(4)	Không.	Không.
FCS_RBG_EXT.1	Không.	Không.
FDP_RIP.2	Không.	Không.
FIA_PMG_EXT.1	Không.	Không.
FIA_UIA_EXT.1	Tất cả sử dụng cơ chế định danh và xác thực.	Định danh người dùng, nguồn gốc của nỗ lực (ví dụ, địa chỉ IP).

FIA_UAU_EXT.2	Tất cả sử dụng cơ chế định danh và xác thực.	Nguồn gốc của nỗ lực (ví dụ, địa chỉ IP).
FIA_UAU.7	Không.	Không.
FIA_X509_EXT.1	Xác thực chứng thư không thành công.	Lý do thất bại.
FIA_X509_EXT.2	Không.	Không.
FIA_X509_EXT.3	Không.	Không.
FMT_MOF.1(1)/ TrustedUpdate	Nỗ lực khởi tạo một cập nhật thủ công.	Không.
FMT_MTD.1	Tất cả các hoạt động quản lý của dữ liệu TSF.	Không.
FMT_SMF.1	Không.	Không.
FMT_SMR.2	Không.	Không.
FPT_SKP_EXT.1	Không.	Không.
FPT_APW_EXT.1	Không.	Không.
FPT_TST_EXT.1	Không.	Không.
FPT_TUD_EXT.1	Bắt đầu cập nhật; kết quả của nỗ lực cập nhật (thành công hay thất bại).	Không có thông tin bổ sung.
FPT_STM.1	Thay đổi thời gian.	Các giá trị cũ và mới cho thời gian. Nguồn gốc của nỗ lực thay đổi thời gian - thành công và thất bại (ví dụ: địa chỉ IP).
FTA_SSL_EXT.1	Nỗ lực mở khóa một phiên tương tác.	Không.
FTA_SSL.3	Kết thúc một phiên từ xa bằng cơ chế khóa phiên.	Không.
FTA_SSL.4	Kết thúc một phiên tương tác.	Không.
FTA_TAB.1	Không.	Không.
FTP_ITC.1	Khởi tạo kênh đáng tin cậy. Kết thúc kênh đáng tin cậy. Sự thất bại của các chức năng của kênh đáng tin cậy.	Xác định bộ khởi tạo và mục tiêu các nỗ lực thiết lập các kênh tin cậy bị thất bại.

FTP_TRP.1	Khởi tạo đường dẫn tin cậy. Kết thúc đường dẫn tin cậy. Sự thất bại của các chức năng đường dẫn tin cậy.	Xác định định danh người dùng đã xác nhận.
FFW_RUL_EXT.1	Áp dụng các qui tắc được cấu hình bằng thao tác "log".	Địa chỉ nguồn và đích; Cổng nguồn và đích; Giao thức tầng giao vận; Giao diện TOE
	Thể hiện các gói tin bị giảm xuống do quá nhiều lưu lượng mạng.	Giao diện TOE không thể xử lý các gói tin; Bộ xác định quy tắc gây ra giảm gói tin.

Chú thích áp dụng: Các sự kiện kiểm toán bổ sung sẽ áp dụng cho TOE tùy thuộc vào các yêu cầu tùy chọn và dựa trên lựa chọn từ Phụ lục A và Phụ lục B. Do đó, tác giả ST phải bao gồm các sự kiện bổ sung có liên quan được xác định trong Bảng 3 và Bảng 4.

Sự kiện kiểm toán đối với FIA_X509_EXT.1 dựa trên TOE không thể hoàn tất việc xác nhận chứng thư bằng cách đảm bảo những điều sau:

- Sự hiện diện của tiện ích mở rộng basicConstraint và CA flag được đặt thành TRUE cho tất cả các chứng thư CA;
- Xác minh chữ ký số của CA có phân cấp đáng tin cậy;
- Đọc/truy cập CRL hoặc truy cập máy chủ OCSP.

Nếu bất kỳ kiểm tra nào thất bại, thì một sự kiện kiểm toán với lỗi đó sẽ được ghi vào nhật ký kiểm toán.

9.3.1.2 FAU_GEN.2 Liên kết định danh người dùng

FAU_GEN.2.1 Đối với các sự kiện kiểm toán phát sinh từ các hành động của người dùng đã được xác định, TSF phải có thể liên kết mỗi sự kiện có thể kiểm toán được với định danh của người dùng tạo ra sự kiện.

9.3.2 Lưu trữ sự kiện kiểm toán an toàn (Extended – FAU_STG_EXT)

Một thiết bị mạng TOE không được kỳ vọng phải chịu trách nhiệm đối với tất cả các lưu trữ kiểm toán. Mặc dù thiết bị được yêu cầu lưu trữ dữ liệu cục bộ tại thời điểm tạo ra dữ liệu kiểm toán, và phải thực hiện một số hành động thích hợp nếu dung lượng lưu trữ cục bộ bị vượt quá, TOE cũng phải có khả năng thiết lập một liên kết an toàn tới máy chủ kiểm toán độc lập để cho phép lưu trữ kiểm toán bên ngoài.

9.3.2.1 FAU_ STG_EXT.1 Lưu trữ sự kiện kiểm toán được bảo vệ

FAU_STG_EXT.1.1 TSF phải có thể truyền dữ liệu kiểm toán đã tạo sang một thực thể CNTT bên ngoài sử dụng một kênh tin cậy theo FTP_ITC.1.

Chú thích áp dụng: Để lựa chọn tùy chọn truyền dữ liệu kiểm toán đã được tạo sang một thực thể CNTT bên ngoài, TOE dựa vào một máy chủ kiểm toán không phải là TOE để lưu trữ và xem lại hồ sơ kiểm toán. Việc lưu trữ các hồ sơ kiểm toán này và khả năng cho phép quản trị viên xem lại hồ sơ kiểm toán được cung cấp bởi môi trường hoạt động trong trường hợp đó.

FAU_STG_EXT.1.2 TSF phải có thể lưu trữ dữ liệu kiểm toán đã tạo lên chính TOE.

FAU_STG_EXT.1.3 TSF phải [lựa chọn: *loại bỏ dữ liệu kiểm toán mới, ghi đè các bản ghi kiểm toán trước đó theo quy tắc sau: [chỉ định: nguyên tắc ghi đè các bản ghi kiểm toán trước đó], [chỉ định: hành động khác]*] khi không gian lưu trữ cục bộ cho dữ liệu kiểm toán đã đầy.

Chú thích áp dụng: Máy chủ đăng nhập bên ngoài có thể được sử dụng làm không gian lưu trữ thay thế trong trường hợp không gian lưu trữ cục bộ đầy. Các "hành động khác" trong trường hợp này có thể được định nghĩa là "gửi ngày kiểm toán mới cho một thực thể CNTT bên ngoài".

9.4 Hỗ trợ mã hóa (FCS)

9.4.1 Quản lý khóa mã hóa (FCS_CKM)

Điều này xác định các yêu cầu về mật mã làm nền tảng cho các thuộc tính bảo mật khác của TOE, bao gồm việc tạo khóa và tạo bit ngẫu nhiên, phương thức thiết lập khóa, hủy khóa và các thao tác mã hóa khác nhau để cung cấp mã hóa/giải mã AES, xác minh chữ ký, tạo giá trị băm, và tạo giá trị băm có khóa.

Các SFR này hỗ trợ việc thực hiện các SFR cấp giao thức dựa trên lựa chọn trong Phụ lục B.

9.4.1.1 FCS_CKM.1 Tạo khóa mã hóa (đã được tinh chỉnh)

FCS_CKM.1.1 TSF sẽ tạo các khóa mã hóa **đối xứng** theo thuật toán tạo khóa mã hóa cụ thể: [lựa chọn:

- ***Các cơ chế RSA sử dụng các kích thước khóa mã hóa 2048 bit hoặc lớn hơn đáp ứng tiêu chuẩn sau: FIPS PUB 186-4, "Tiêu chuẩn Chữ ký số (DSS)", Phụ lục B.3;***
- ***Cơ chế ECC sử dụng "NIST curves" [Lựa chọn: P-256, P-384, P-521] đáp ứng tiêu chuẩn sau: FIPS PUB 186-4, "Tiêu chuẩn Chữ ký số (DSS)", Phụ lục B.4;***
- ***Cơ chế FFC sử dụng các kích thước khóa mã hóa 2048 bit hoặc lớn hơn đáp ứng tiêu chuẩn sau: FIPS PUB 186-4, "Tiêu chuẩn Chữ ký số (DSS)", Phụ lục B.1***

] ~~*Và các kích thước mã hóa cụ thể* [chỉ định: kích thước khóa mã hóa] đáp ứng tiêu chuẩn sau: [chỉ định: *danh sách các tiêu chuẩn*].~~

Chú thích áp dụng: Tác giả ST chọn tất cả các cơ chế tạo khóa được sử dụng để thiết lập khóa và xác thực thiết bị. Khi tạo khóa được sử dụng để thiết lập khóa, các lược đồ trong FCS_CKM.2.1 và các

giao thức mã hóa được chọn phải phù hợp với sự lựa chọn. Khi tạo khóa được sử dụng để xác thực thiết bị, khóa công khai dự kiến sẽ được liên kết với một chứng thư X.509v3.

Nếu TOE hoạt động như một đối tượng tiếp nhận trong lược đồ thiết lập khóa RSA, TOE không cần phải thực hiện việc tạo khóa RSA.

9.4.1.2 FCS_CKM.2 Thiết lập khóa mã hóa (đã được tinh chỉnh)

FCS_CKM.2.1 TSF sẽ thực **hiện việc thiết lập khóa** mã hóa theo một phương pháp thiết lập khóa mã hóa cụ thể: [lựa chọn:

- ***Các lược đồ thiết lập khóa dựa trên RSA đáp ứng các yêu cầu sau: NIST SP 800-56B, "Đề xuất dành cho các lược đồ lập khóa theo cặp sử dụng phương pháp tìm thừa số nguyên tố";***
- ***Các lược đồ thiết lập khóa dựa trên đường cong Elliptic đáp ứng các yêu cầu sau: NIST SP 800-56A, "Đề xuất dành cho các lược đồ thiết lập khóa theo cặp sử dụng Thuật toán logarit rời rạc";***
- ***Các lược đồ thiết lập khóa dựa trên trường xác định đáp ứng các yêu cầu sau: NIST SP 800-56A, "Đề xuất dành cho các lược đồ thiết lập khóa theo cặp sử dụng Thuật toán logarit rời rạc"***

] ~~đáp ứng nội dung sau: [chỉ định: *danh sách các tiêu chuẩn*]~~.

Chú thích áp dụng: Đây là SFR FCS_CKM.2 tinh chỉnh để giải quyết việc thiết lập khóa chứ không phải là phân phối khóa.

Tác giả ST chọn tất cả các lược đồ thiết lập khóa được sử dụng cho các giao thức mã hóa đã được chọn.

Các lược đồ thiết lập khóa dựa trên RSA được mô tả trong điều 9 của NIST SP 800-56B; tuy nhiên, điều 9 dựa vào việc thực hiện các điều khác trong SP 800-56B. Nếu TOE hoạt động như một bộ phận tiếp nhận trong lược đồ thiết lập khóa RSA, thì TOE không cần phải thực hiện việc tạo khóa RSA.

Các đường cong Elliptic được sử dụng cho lược đồ thiết lập khóa tương quan với các đường cong được xác định trong FCS_CKM.1.1.

Các thông số về tên miền được sử dụng cho lược đồ thiết lập khóa dựa trên trường xác định được quy định cụ thể bằng tạo khóa theo FCS_CKM.1.1.

9.4.1.3 FCS_CKM.4 Phá hủy khóa mã hóa

FCS_CKM.4.1 TSF phải phá hủy các khóa mã hóa theo một phương pháp phá hủy được xác định cụ thể *[lựa chọn:*

- *Đối với bộ nhớ tạm thời, việc phá hủy khóa sẽ được thực hiện bằng cách ghi đè trực tiếp [lựa chọn: bao gồm một mẫu (pattern) giả ngẫu nhiên sử dụng RBG của TSF, bao gồm các số không] và theo sau là một quá trình read-verify (đọc-xác minh).*
    - *Nếu việc đọc-xác minh dữ liệu được ghi đè thất bại, thì quá trình sẽ được lặp lại.*

- *Đối với EEPROM điện tĩnh, sự phá hủy sẽ được thực hiện bằng cách ghi đè trực tiếp, bao gồm một mẫu giả ngẫu nhiên sử dụng RBG của TSF (như đã nêu trong FCS_RBG_EXT.1), sau đó là quá trình đọc- xác minh.*
    - *Nếu việc đọc-xác minh dữ liệu được ghi đè thất bại, thì quá trình sẽ được lặp lại.*
- *Đối với bộ nhớ flash điện tĩnh, việc phá hủy khóa sẽ được thực hiện bằng cách [lựa chọn: ghi đè trực tiếp bao gồm các số không, xóa khối] và theo sau là một quá trình read-verify (đọc-xác minh).*
    - *Nếu việc đọc-xác minh dữ liệu được ghi đè thất bại, thì quá trình sẽ được lặp lại.*
- *Đối với bộ nhớ điện tĩnh khác với EEPROM và bộ nhớ flash, việc phá hủy khóa sẽ được thực hiện bằng cách ghi đè lên ba lần hoặc nhiều lần bằng một mẫu ngẫu nhiên được thay đổi trước mỗi lần ghi.*

]

Đáp ứng tiêu chuẩn sau: *Không tiêu chuẩn.*

9.4.2 Thao tác mã hóa (FCS_COP)

9.4.2.1 FCS_COP.1 Thao tác mã hóa

FCS_COP.1.1(1) TSF phải thực hiện *mã hóa/giải mã* theo một thuật toán mã hóa AES cụ thể *được sử dụng trong chế độ* [*lựa chọn*: CBC, GCM] và các kích thước khóa mã hóa [*lựa chọn: 128 bit, 192 bit, 256 bit*] đáp ứng các tiêu chuẩn sau: AES theo qui định trong ISO 18033-3, [*lựa chọn: CBC theo quy định của ISO 10116, GCM theo qui định trong ISO 19772*].

Chú thích áp dụng: Đối với lựa chọn đầu tiên của FCS_COP.1.1 (1), tác giả ST nên chọn chế độ hoặc các chế độ có AES hoạt động. Đối với lựa chọn thứ hai, tác giả ST nên chọn các kích thước khóa được hỗ trợ bởi chức năng này. Các chế độ và kích thước khóa được chọn ở đây tương ứng với các lựa chọn của bộ giải mã được thực hiện theo các yêu cầu kênh đáng tin cậy.

FCS_COP.1.1(2) TSF phải thực hiện các dịch vụ chữ ký mã hóa (tạo và xác thực) theo thuật toán mã hóa cụ thể [lựa chọn:

- *Thuật toán Chữ ký số RSA và các kích thước khóa mã hóa (mô-đun) [chỉ định: 2048 bit hoặc lớn hơn],*
- *Thuật toán Chữ ký số đường cong Elliptic và các kích thước khóa mã hóa [chỉ định: 256 bit hoặc lớn hơn]*

]

Đáp ứng các tiêu chuẩn sau: [lựa chọn:

- *Đối với các lược đồ RSA: FIPS PUB 186-4, "Tiêu chuẩn chữ ký số (DSS)", Điều 5.5, sử*

dụng PKCS #1 v2.1 Các lược đồ chữ ký RSASSA-PSS và/hoặc RSASSA- PKCS2v1_5; ISO/IEC 9796-2, Lược đồ chữ ký số 2 hoặc Lược đồ chữ ký số 3,

- *Đối với lược đồ ECDSA: FIPS PUB 186-4, "Tiêu chuẩn chữ ký số (DSS)", Điều 6 và Phụ lục D, thực hiện "các đường cong NIST" P-256, P-384, và [lựa chọn: P- 521, không đường cong nào khác]; ISO/IEC 14888-3, Điều 6.4*

].

Chú thích áp dụng: Tác giả ST nên chọn thuật toán đã được thực hiện để tạo chữ ký số. Đối với (các) thuật toán đã chọn, tác giả ST nên thực hiện các chỉ định/lựa chọn thích hợp để xác định các tham số được thực hiện cho thuật toán đó.

FCS_COP.1.1(3) TSF phải thực hiện các dịch vụ băm mã hóa theo một thuật toán mã hóa cụ thể [*lựa chọn: SHA-1, SHA-256, SHA-384, SHA-512, không có các thuật toán khác*] ~~và các kích thước khóa mã hóa [chỉ định: các kích thước khóa mã hóa]~~ đáp ứng tiêu chuẩn sau: ISO/IEC 10118-3:2004.

Chú thích áp dụng: Các nhà cung cấp được khuyến khích thực hiện các giao thức cập nhật hỗ trợ hệ SHA-2; cho đến khi các giao thức được cập nhật được hỗ trợ, tiêu chuẩn này cho phép hỗ trợ cho việc triển khai SHA-1 phù hợp với SP 800-131A.

Lựa chọn băm phải phù hợp với sức mạnh tổng thể của thuật toán được sử dụng cho FCS_COP.1 (1) và FCS_COP.1 (2) (ví dụ: SHA 256 cho các khóa 128-bit).

FCS_COP.1.1(4) TSF phải thực hiện *xác thực tin báo băm-đã khóa* theo một thuật toán mã hóa xác định *[lựa chọn: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512]* và các kích thước khóa mã hóa [chỉ định: kích thước khóa (theo bit) được sử dụng trong HMAC] và **kích cỡ tóm lược tin báo** ***[lựa chọn: 160, 256, 384, 512]*** **bit** đáp ứng các tiêu chuẩn sau đây: *ISO/IEC 9797-2: 2011, điều 7 "Thuật toán MAC 2".*

Chú thích áp dụng: Kích thước khóa [k] trong chỉ định rơi vào khoảng giữa L1 và L2 (được xác định trong ISO/IEC 10118 cho hàm băm thích hợp). Ví dụ: đối với SHA-256, L1 = 512, L2 = 256, trong đó L2 <= k <= L1.

9.4.3 Bộ sinh bit ngẫu nhiên (Extended – FCS_RBG_EXT)

9.4.3.1 FCS_RBG_EXT.1 Bộ sinh bit ngẫu nhiên

FCS_RBG_EXT.1.1 TSF phải thực hiện các dịch vụ tạo bit ngẫu nhiên theo ISO/IEC 18031:2011 sử dụng [lựa chọn: *Hash_DRBG (bất kỳ), HMAC_DRBG (bất kỳ), CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 RBG xác định sẽ được gieo (seeded) bởi ít nhất một nguồn entropy mà tích lũy entropy từ [lựa chọn: *[chỉ định: số lượng nguồn dựa trên phần mềm] nguồn nhiễu dựa trên phần mềm,, [chỉ định: số lượng nguồn dựa trên phần cứng] nguồn nhiễu dựa trên phần cứng*] với mức tối thiểu là [lựa chọn *128 bit, 192 bit, 256 bit*] của entropy tối thiểu bằng độ với độ mạnh an toàn lớn nhất, theo

ISO/IEC 18031: 2011 Bảng C.1 "Bảng Độ mạnh an toàn cho hàm băm", của các khóa và băm mà nó sẽ tạo ra.

Chú thích áp dụng: Đối với lựa chọn đầu tiên trong FCS_RBG_EXT.1.2, ST chọn ít nhất một trong số các loại nguồn nhiễu. Nếu TOE chứa nhiều nguồn nhiễu cùng loại, thì tác giả ST sẽ cho vào chỉ định với số lượng thích hợp cho từng loại nguồn (ví dụ: 2 nguồn nhiễu dựa trên phần mềm, 1 nguồn nhiễu dựa trên phần cứng). Các tài liệu và các bài thử nghiệm được yêu cầu trong hoạt động đánh giá cho thành phần này nhất thiết phải bao gồm mỗi nguồn được chỉ định trong ST.

ISO/IEC 18031:2011 chứa ba phương pháp tạo các số ngẫu nhiên khác nhau; mỗi một phương pháp phụ thuộc vào các cryptographic primitive (mã hóa nguyên thủy) cơ bản (các hàm băm/mật mã). Tác giả ST sẽ chọn hàm được sử dụng, và đưa các cryptographic primitive cơ bản được sử dụng trong yêu cầu. Mặc dù các hàm băm đã xác định (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) được cho phép đối với Hash_DRBG hoặc HMAC_DRBG, nhưng chỉ các triển khai dựa trên AES đối với CTR_DRBG là được phép.

Nếu chiều dài khóa cho việc triển khai AES được sử dụng ở đây khác với chiều dài được sử dụng để mã hóa dữ liệu người dùng thì FCS_COP.1 có thể phải được điều chỉnh hoặc lặp lại để phản ánh độ dài khóa khác nhau. Đối với việc lựa chọn trong FCS_RBG_EXT.1.2, tác giả ST chọn số bit tối thiểu của entropy được sử dụng để gieo (seed) RBG.

9.5 Bảo vệ dữ liệu người dùng (FDP)

Điều này yêu cầu TOE đảm bảo rằng nó không sử dụng lại gói thông tin cũ khi truyền gói mới.

9.5.1 Bảo vệ thông tin dư thừa (FDP_RIP)

9.5.1.1 FDP_RIP.2 Bảo vệ thông tin dư thừa hoàn toàn

FDP_RIP.2.1 TSF phải đảm bảo rằng bất kỳ nội dung thông tin trước đó của một tài nguyên sẽ không còn khả dụng khi [*lựa chọn: phân bổ tài nguyên tới, giải phóng tài nguyên đã cấp cho*] tất cả các đối tượng.

Chú thích áp dụng: "Tài nguyên" trong bối cảnh của yêu cầu này là các gói tin mạng được gửi qua TOE (trái ngược với "đến", như trường hợp khi một quản trị viên an toàn kết nối với TOE). Mối quan tâm ở đây là khi một gói tin mạng được gửi đi, bộ đệm hoặc vùng bộ nhớ được gói tin sử dụng vẫn chứa dữ liệu từ gói đó, và nếu bộ đệm đó được sử dụng lại thì những dữ liệu đó có thể vẫn còn và đi vào một gói tin mới.

9.6 Định danh và xác thực (FIA)

Để cung cấp một phương tiện đáng tin cậy cho các quản trị viên tương tác với TOE, TOE cung cấp cơ chế đăng nhập dựa trên mật khẩu. Quản trị viên phải có khả năng soạn một mật khẩu mạnh và có các cơ chế để mật khẩu phải được thay đổi thường xuyên. Để tránh các cuộc tấn công mà kẻ tấn công có

thể quan sát được khi quản trị viên đang gõ mật khẩu, mật khẩu phải được che khuất trong quá trình đăng nhập. Khóa hoặc kết thúc phiên cũng phải được thực hiện để giảm thiểu nguy cơ một tài khoản đang được sử dụng bất hợp pháp. Mật khẩu phải được lưu trữ dưới dạng bị che khuất và không có giao thức nào được cung cấp để đọc mật khẩu hoặc tệp mật khẩu khi hiển thị dưới dạng bản rõ.

9.6.1 Quản lý mật khẩu (Extended – FIA_PMG_EXT)

9.6.1.1 FIA_PMG_EXT.1 Quản lý mật khẩu

FIA_PMG_EXT.1.1 TSF phải cung cấp các khả năng quản lý mật khẩu dưới đây dành cho các mật khẩu của quản trị viên:

a) Mật khẩu có thể bao gồm các kết hợp từ các chữ hoa và chữ thường, số và các ký tự đặc biệt sau đây: [chọn: "!", "@", "#", "$", "%" "^", "&", "", "(", ")", [chỉ định: các ký tự khác]];*

b) Chiều dài mật khẩu tối thiểu phải được quản trị viên an toàn xác định và phải hỗ trợ mật khẩu từ 15 ký tự trở lên.

Chú thích áp dụng: Tác giả ST chọn các ký tự đặc biệt được hỗ trợ bởi TOE; họ có thể tùy ý liệt kê các ký tự đặc biệt bổ sung được hỗ trợ bằng cách sử dụng chỉ định. "Mật khẩu quản trị" đề cập đến các mật khẩu được quản trị viên sử dụng tại bảng điều khiển cục bộ, qua các giao thức hỗ trợ mật khẩu, chẳng hạn như SSH và HTTPS, hoặc cấp dữ liệu cấu hình hỗ trợ các SFR khác trong ST.

9.6.2 Định danh và xác thực người dùng (Extended – FIA_UIA_EXT)

9.6.2.1 FIA_UIA_EXT.1 Định danh và xác thực người dùng

FIA_UIA_EXT.1.1 TSF phải cho phép các hành động sau đây trước khi yêu cầu các thực thể không phải là TOE khởi tạo quá trình định danh và xác thực:

- Hiển thị banner cảnh báo theo FTA_TAB.1;
- [lựa chọn: *không các hành động khác, [chỉ định: danh sách các dịch vụ, các hành động được thực hiện bởi TSF để đáp ứng các yêu cầu không phải TOE.*]

FIA_UIA_EXT.1.2 TSF phải yêu cầu mỗi người dùng quản trị được định danh và xác thực thành công trước khi cho phép bất kỳ hành động nào làm TSF trung gian thay mặt cho người dùng quản trị đó.

Chú thích áp dụng: Yêu cầu này áp dụng cho người dùng (các quản trị viên và các đơn vị CNTT bên ngoài) các dịch vụ có sẵn trực tiếp từ TOE, và không phải các dịch vụ có sẵn bằng cách kết nối thông qua TOE. Trong trường hợp có ít hoặc không có dịch vụ nào có sẵn cho các đơn vị bên ngoài trước khi định danh và xác thực, nếu có một số có sẵn (có thể là ICMP echo), thì chúng phải được liệt kê trong câu lệnh chỉ định; nếu không "không có hành động khác" được lựa chọn.

Xác thực có thể dựa trên mật khẩu thông qua bảng điều khiển cục bộ hoặc thông qua giao thức hỗ trợ mật khẩu (như SSH) hoặc dựa trên chứng thư (như SSH, TLS).

Đối với các giao tiếp với các thực thể CNTT bên ngoài (ví dụ: máy chủ kiểm toán hoặc máy chủ NTP), các kết nối như vậy phải được thực hiện theo FTP_ITC.1, có giao thức thực hiện định danh và xác thực. Điều này có nghĩa là các giao tiếp như vậy (ví dụ, thiết lập kết nối IPsec tới máy chủ xác thực) sẽ không được xác định cụ thể trong chỉ định, do việc thiết lập kết nối "tăng số đếm" mỗi khi khởi động quá trình định danh và xác thực.

9.6.3 Xác thực người dùng (FIA_UAU) (Extended – FIA_UAU_EXT)

9.6.3.1 FIA_UAU_EXT.2 Cơ chế xác thực dựa trên mật khẩu

FIA_UAU_EXT.2.1 TSF phải cung cấp cơ chế xác thực dựa trên mật khẩu cục bộ, *[lựa chọn: [chỉ định: cơ chế xác thực khác], không]* để thực hiện xác thực người dùng quản trị.

Chú thích áp dụng: Chỉ định cần được sử dụng để xác định bất kỳ cơ chế xác thực cục bộ bổ sung nào được hỗ trợ. Các cơ chế xác thực cục bộ được định nghĩa là các cơ chế xác thực cục bộ xảy ra thông qua bảng điều khiển cục bộ; các phiên quản trị từ xa (và các cơ chế xác thực liên quan) được quy định trong FTP_TRP.1.

9.6.3.2 FIA_UAU.7 Phản hồi xác thực được bảo vệ

FIA_UAU.7.1 TSF chỉ cung cấp *phản hồi bị che khuất* cho người dùng quản trị trong khi quá trình xác thực đang được tiến hành tại bảng điều khiển cục bộ.

Chú thích áp dụng: "Phản hồi bị che khuất "có nghĩa là TSF không hiển thị bất kỳ dữ liệu xác thực nào được nhập bởi người dùng (ví dụ như phản hồi của mật khẩu) mặc dù chỉ báo về tiến độ xác thực có thể được cung cấp (như dấu hoa thị cho mỗi ký tự). Điều này cũng ngụ ý rằng TSF không phản hồi bất kỳ thông tin nào trong quá trình xác thực tới người dùng mà chỉ có thể cung cấp dấu hiệu về dữ liệu xác thực.

9.6.4 Xác thực sử dụng các chứng thư X.509 (Extended – FIA_X509_EXT)

9.6.4.1 FIA_X509_EXT.1 Xác nhận chứng thư X.509

FIA_X509_EXT.1.1 TSF phải xác nhận chứng thư theo các quy tắc sau

- Xác nhận chứng thư RFC 5280 và xác nhận đường dẫn chứng thư.
- Đường dẫn chứng thư phải kết thúc bằng một chứng thư CA tin cậy.
- TSF sẽ xác nhận đường dẫn chứng thư bằng cách đảm bảo sự hiện diện của phần mở rộng basicConstraints và flag CA được cài đặt thành TRUE cho tất cả các chứng thư CA.
- TSF sẽ xác nhận tình trạng thu hồi giấy chứng thư bằng cách sử dụng [lựa chọn: *Giao thức trạng thái chứng thư trực tuyến (OCSP) theo quy định tại RFC 2560, một danh sách thu hồi chứng thư (CRL) như đã quy định trong RFC 5759*].
- TSF sẽ xác nhận extendedKeyUsage theo các quy tắc sau:

- *Các chứng thư được sử dụng cho các cập nhật tin cậy và xác minh tính hợp mã thực thi sẽ có mục đích Ký hiệu mã (id-kp 3 với OID 1.3.6.1.5.5.7.3.3) trong trường extendedKeyUsage.*
- *Các chứng thư máy chủ được trình bày cho TLS sẽ có mục đích Xác thực Máy chủ (id-kp 1 với OID 1.3.6.1.5.5.7.3.1) trong trường extendedKeyUsage.*
- *Các chứng thư máy khách được trình bày cho TLS phải có mục đích Xác thực Khách hàng (id-kp 2 với OID 1.3.6.1.5.5.7.3.2) trong trường extendedKeyUsage.*
- *Các chứng thư OCSP được trình bày cho các phản hồi của OCSP sẽ có mục đích Đăng ký OCSP (id-kp 9 với OID 1.3.6.1.5.5.7.3.9) trong trường extendedKeyUsage.*

Chú thích áp dụng: FIA_X509_EXT.1.1 liệt kê các quy tắc để xác nhận chứng thư. Tác giả ST lựa chọn xem trạng thái thu hồi có được xác minh bằng cách sử dụng OCSP hay các CRL hay không. Các giao thức kênh/đường dẫn đáng tin cậy yêu cầu chứng thư được sử dụng; việc sử dụng này yêu cầu các quy tắc extendedKeyUsage được xác minh.

Việc xác nhận hợp lệ dự kiến sẽ kết thúc bằng một chứng thư CA gốc đáng tin cậy trong một nơi lưu trữ gốc được quản lý bởi nền tảng.

FIA_X509_EXT.1.2 TSF chỉ coi một chứng thư như là một chứng thư CA nếu basicConstraints và flag CA được cài đặt thành TRUE.

Chú thích áp dụng: Yêu cầu này áp dụng cho các chứng thư được TSF sử dụng và xử lý và hạn chế các chứng thư có thể được bổ sung làm chứng thư CA đáng tin cậy.

9.6.4.2 FIA_X509_EXT.2 Xác thực chứng thư X.509

FIA_X509_EXT.2.1 TSF phải sử dụng chứng thư X.509v3 theo định nghĩa bởi RFC 5280 để hỗ trợ xác thực cho [lựa chọn: *IPsec, TLS, HTTPS, SSH*] và [lựa chọn: *code signing cho các bản cập nhật phần mềm hệ thống, code signing để xác minh tính toàn vẹn, [chỉ định: sử dụng khác], không sử dụng thêm*].

Chú thích áp dụng: Sự lựa chọn của tác giả ST phù hợp với lựa chọn của FTP_ITC.1.1. Các chứng thư có thể được tùy chọn sử dụng cho các cập nhật phần mềm hệ thống (FPT_TUD_EXT.1) và để xác minh tính toàn vẹn (FPT_TST_EXT.2).

FILE_X509_EXT.2.2 Khi TSF không thể thiết lập kết nối để xác định tính hợp lệ của chứng thư, TSF sẽ [lựa chọn: *cho phép quản trị viên chọn chấp nhận chứng thư trong các trường hợp này, chấp nhận chứng thư, không chấp nhận chứng thư*].

Chú thích áp dụng: Thông thường một kết nối phải được thiết lập để kiểm tra tình trạng thu hồi của một chứng thư – kể cả tải một CRL hay thực hiện tra cứu bằng cách sử dụng OCSP. Lựa chọn được sử dụng để mô tả hành vi trong trường hợp không thể thiết lập kết nối như vậy (ví dụ do lỗi mạng). Nếu TOE đã xác định chứng thư hợp lệ theo tất cả các quy tắc khác trong FIA_X509_EXT.1, thì hành vi được thể hiện trong lựa chọn sẽ xác định tính hợp lệ. TOE không được chấp nhận chứng thư nếu nó

không tuân thủ bất kỳ quy tắc xác nhận hợp lệ nào khác trong FIA_X509_EXT.1. Nếu tùy chọn quản trị viên cấu hình được chọn bởi tác giả ST, thì tác giả ST cũng chọn chức năng tương ứng trong FMT_SMF.1.

9.6.4.3 FIA_X509_EXT.3 Yêu cầu chứng thư X.509

FIA_X509_EXT.3.1 TSF phải tạo ra một Thông báo yêu cầu chứng thư theo quy định của RFC 2986 và có thể cung cấp các thông tin sau trong yêu cầu: khóa công khai và [lựa chọn: *thông tin về thiết bị cụ thể, Tên thường, Tổ chức, Đơn vị Tổ chức, Quốc gia*].

Chú thích áp dụng: Khóa công khai là phần khóa công khai của cặp khóa công khai - khóa riêng được tạo ra bởi TOE như quy định trong FCS_CKM.1 (1).

FIA_X509_EXT.3.2 TSF phải xác nhận chuỗi chứng thư từ CA gốc khi nhận được Phản hồi chứng thư CA.

9.7 Quản lý an toàn (FMT)

Các chức năng quản lý được yêu cầu trong điều này mô tả các khả năng cần thiết để hỗ trợ vai trò quản trị viên an toàn và bộ các chức năng quản lý an toàn cơ bản để quản lý các khía cạnh có thể cấu hình có trong các SFR khác (FMT_SMF.1), quản lý chung dữ liệu TSF (FMT_MTD.1), và cho phép các cập nhật TOE (FMT_MOF.1 (1) / Cập nhật tin cậy).

Các yêu cầu quản lý cốt lõi này được bổ sung bởi các yêu cầu tùy chọn trong điều A.3 và các yêu cầu dựa trên lựa chọn trong điều B.4, theo các khả năng của TOE.

9.7.1 Quản lý các chức năng trong TSF (FMT_MOF)

9.7.1.1 FMT_MOF.1(1)/TrustedUpdate Quản lý hành vi các chức năng an toàn

FMT_MOF.1.1(1)/TrustedUpdate TSF phải hạn chế khả năng kích hoạt các chức năng *cập nhật thủ công cho các quản trị viên an toàn.*

Chú thích áp dụng: FMT_MOF.1(1)/TrustedUpdate hạn chế việc khởi tạo cập nhật thủ công bởi các quản trị viên an toàn.

9.7.2 Quản lý dữ liệu TSF (FMT_MTD)

9.7.2.1 FMT_MTD.1 Quản lý dữ liệu TSF

FMT_MTD.1.1 TSF phải giới hạn khả năng quản lý *dữ liệu TSF* cho các *quản trị viên an toàn.*

Chú thích áp dụng: Từ "quản lý" bao gồm nhưng không giới hạn trong việc tạo, khởi tạo, xem, thay đổi mặc định, sửa đổi, xóa, và nối thêm. SFR này bao gồm cả việc cài đặt lại mật khẩu người dùng bởi quản trị viên an toàn.

9.7.3 Đặc tả của các chức năng quản lý (FMT_SMF)

9.7.3.1 FMT_SMF.1 Đặc tả của các chức năng quản lý

FMT_SMF.1.1 TSF phải có khả năng thực hiện các chức năng quản lý sau:

- *Khả năng quản lý TOE cục bộ và từ xa;*
- *Khả năng cấu hình các banner truy cập;*
- *Khả năng cấu hình thời gian không hoạt động của phiên trước khi kết thúc hoặc khóa phiên;*
- *Khả năng cập nhật TOE, và xác minh các bản cập nhật sử dụng khả năng chữ ký số trước khi cài đặt những bản cập nhật;*
- *Khả năng cấu hình các quy tắc tường lửa;*
- *[lựa chọn:*
    - *Khả năng cấu hình hành vi kiểm toán;*
    - *Khả năng cấu hình danh sách các dịch vụ TOE cung cấp sẵn có trước khi một thực thể được định danh và xác thực, như quy định trong FIA_UIA_EXT.1;*
    - *Khả năng cấu hình các chức năng mã hóa;*
    - *Không có khả năng khác.]*

Chú thích áp dụng: TOE phải cung cấp chức năng cho cả quản trị cục bộ và từ xa, bao gồm khả năng định cấu hình biểu ngữ truy cập cho FTA_TAB.1 và thời gian không hoạt động của phiên cho FTA_SSL.3 & FTA_SSL.4. Điều "Khả năng cập nhật TOE, và xác minh các bản cập nhật sử dụng khả năng chữ ký số trước khi cài đặt những bản cập nhật" bao gồm các chức năng quản lý có liên quan từ FMT_MOF.1 (1) / TrustedUpdate, FMT_MOF.1 (2) / TrustedUpdate (nếu có trong ST), FIA_X509_EXT.2.2 và FPT_TUD_EXT.2.2 (nếu có trong ST và nếu chúng bao gồm hành động cấu hình của quản trị viên). Tương tự, lựa chọn "Khả năng cấu hình hành vi kiểm toán" bao gồm các chức năng quản lý có liên quan từ FMT_MOF.1 (1) / audit, FMT_MOF.1 (2) / audit, FMT_MOF.1.1 (1) / AdminAct, FMT_MOF.1.1 (2) / AdminAct và FMT_MOF.1 / LocSpace (đối với tất cả các SFR có trong ST). Nếu TOE cung cấp khả năng cho quản trị viên cấu hình hành vi kiểm toán, cấu hình các dịch vụ sẵn có trước khi định danh hoặc xác thực, hoặc nếu bất kỳ chức năng mã hóa nào trên TOE có thể được cấu hình, thì tác giả ST đưa ra lựa chọn hoặc các lựa chọn thích hợp trong phần lựa chọn thứ hai, nếu không thì chọn "Không có khả năng khác."

9.7.4 Vai trò quản lý an toàn (FMT_SMR)

9.7.4.1 FMT_SMR.2 Các giới hạn đối với các vai trò an toàn

FMT_SMR.2.1 The TSF phải duy trì các vai trò:

- *Quản trị viên an toàn.*

FMT_SMR.2.2 TSF phải có thể liên kết người dùng với vai trò.

FMT_SMR.2.3 TSF phải đảm bảo rằng các điều kiện

- *Vai trò quản trị viên an toàn sẽ có thể quản lý TOE cục bộ;*
- *Vai trò quản trị viên an toàn sẽ có thể quản lý TOE từ xa;*

được đáp ứng.

Chú thích áp dụng: FMT_SMR.2.3 yêu cầu quản trị viên an toàn có thể quản lý TOE thông qua bảng điều khiển cục bộ và thông qua cơ chế từ xa (IPsec, SSH, TLS, TLS / HTTPS).

9.8 Bảo vệ TSF (FPT)

Điều này xác định các yêu cầu cho TOE để bảo vệ các dữ liệu an toàn quan trọng như khóa và mật khẩu, cung cấp các tự kiểm tra để theo dõi hoạt động chính xác liên tục của TOE (bao gồm phát hiện các lỗi của phần sụn hoặc tính toàn vẹn phần mềm) và cung cấp các phương pháp đáng tin cậy cho các bản cập nhật cho phần mềm/phần sụn TOE. Ngoài ra, TOE được yêu cầu cung cấp dấu thời gian (timestamp) đáng tin cậy để hỗ trợ lưu hồ sơ kiểm toán chính xác theo họ FAU_GEN.

9.8.1 Bảo vệ dữ liệu TSF (Extended – FPT_SKP_EXT)

9.8.1.1 FPT_SKP_EXT.1 Bảo vệ dữ liệu TSF (để đọc tất cả khóa đối xứng)

FPT_SKP_EXT.1.1 TSF phải ngăn không cho đọc tất cả các khóa được chia sẻ trước, các khóa đối xứng và các khóa cá nhân.

Chú thích áp dụng: Mục đích của yêu cầu này là để thiết bị bảo vệ khóa, tài liệu quan trọng và các ủy nhiệm xác thực khỏi bị tiết lộ trái phép. Dữ liệu này chỉ nên được truy cập cho các mục đích liên quan đến chức năng an toàn được chỉ định và không cần phải được hiển thị/truy cập ở các thời điểm khác. Yêu cầu này không ngăn thiết bị có các chỉ báo về sự tồn tại, đang được sử dụng hoặc đang còn hiệu lực của các dữ liệu này.

9.8.2 Bảo vệ mật khẩu quản trị viên (Extended – FPT_APW_EXT)

9.8.2.1 FPT_APW_EXT.1 Bảo vệ mật khẩu quản trị viên

FPT_APW_EXT.1.1 TSF phải lưu trữ mật khẩu ở dạng không phải là bản rõ.

FPT_APW_EXT.1.2 TSF phải ngăn chặn việc đọc các mật khẩu dạng bản rõ.

Chú thích áp dụng: Mục đích của yêu cầu là dữ liệu xác thực mật khẩu thô không được lưu trữ dưới dạng các thông tin rõ ràng, và không có người dùng hoặc quản trị viên nào có thể đọc được mật khẩu dạng bản rõ thông qua các giao thức "bình thường". Một quản trị viên nắm quyền quản trị cao nhất của quá trình tất nhiên có thể đọc trực tiếp bộ nhớ để lấy mật khẩu nhưng được tin tưởng là sẽ không làm như vậy.

9.8.3 Thử TSF (Extended – FPT_TST_EXT)

Để phát hiện một số lỗi của các cơ chế an toàn tiềm ẩn được sử dụng bởi TSF, TSF sẽ thực hiện tự kiểm tra. Mức độ tự kiểm tra này được dành cho nhà phát triển sản phẩm, tuy nhiên, một bộ tự kiểm tra toàn diện hơn sẽ tạo ra một nền tảng đáng tin cậy hơn để phát triển phần mềm Enterprise Architect.

(Đối với thành phần này, các yêu cầu dựa trên lựa chọn được trình bày ở Phụ lục B)

9.8.3.1 FPT_TST_EXT.1 Thử TSF (được mở rộng)

FPT_TST_EXT.1.1 TSF phải chạy một bộ tự kiểm tra: [lựa chọn: *khi khởi động ban đầu (bật nguồn), định kỳ trong quá trình hoạt động bình thường, theo yêu cầu của người dùng được ủy quyền, tại các điều kiện [chỉ định: các điều kiện mà tự kiểm tra nên thực hiện]]* để chứng minh hoạt động chính xác của TSF: *[chỉ định: danh sách các bài tự kiểm tra do TSF thực hiện].*

Chú thích áp dụng 1: Điều mong đợi là các bài tự kiểm tra được thực hiện trong quá trình khởi động ban đầu (khi bật nguồn). Các tùy chọn khác chỉ nên được sử dụng nếu nhà phát triển có thể giải thích lý do tại sao chúng không được thực hiện trong quá trình khởi động ban đầu. Các bài tự kiểm tra để xác minh tính toàn vẹn của phần mềm và phần sụn cũng như hoạt động chính xác của các hàm mã hóa cần thiết để đáp ứng các SFR được kỳ vọng ít nhất phải được thực hiện. Nếu không phải tất cả các bài tự kiểm tra được thực hiện trong thời gian khởi động thì cần lặp lại nhiều lần các SFR với các tùy chọn thích hợp được chọn. Trong các phiên bản sau này của tiêu chuẩn này, các tự kiểm tra sẽ được yêu cầu phải có ít nhất các cơ chế để khởi động có đo lường bao gồm các bài tự kiểm tra các thành phần có đo lường.

Chú thích áp dụng 2: Nếu chứng thư được sử dụng bởi cơ chế tự kiểm tra (ví dụ để xác minh chữ ký để xác minh tính toàn vẹn), các chứng thư sẽ được xác thực theo FIA_X509_EXT.1 và phải được chọn trong FIA_X509_EXT.2.1. Thêm vào đó, FPT_TST_EXT.2 phải được đưa vào ST.

9.8.4 Cập nhật tin cậy (FPT_TUD_EXT)

Quản trị viên không thể xác minh được các bản cập nhật cho hệ thống được tin cậy có thể dẫn đến làm hỏng toàn bộ hệ thống. Để tạo độ tin cậy vào nguồn cập nhật, hệ thống có thể cung cấp các cơ chế và thủ tục mã hóa để thu nhận bản cập nhật, kiểm tra bản cập nhật thông qua cơ chế chữ ký số được cung cấp bởi TOE và cài đặt bản cập nhật trên hệ thống. Mặc dù không có yêu cầu rằng quá trình này được tự động hoàn toàn, tuy nhiên, tài liệu hướng dẫn sẽ nêu chi tiết các thủ tục phải được thực hiện thủ công, cũng như cách thức quản trị viên bảo đảm được chữ ký trên bản cập nhật là hợp lệ.

(Đối với họ này, các yêu cầu dựa trên lựa chọn được trình bày ở Phụ lục B)

9.8.4.1 FPT_TUD_EXT.1 Cập nhật tin cậy

FPT_TUD_EXT.1.1 TSF phải cung cấp cho *quản trị viên an toàn* khả năng truy vấn phiên bản thực hiện hiện tại của phần mềm/phần sụn TOE cũng như phiên bản phần mềm/phần sụn TOE được cài đặt gần đây nhất

Chú thích áp dụng: Phiên bản hiện đang chạy (đang được thực thi) có thể không phải là phiên bản được cài đặt gần đây nhất. Ví dụ, có thể là bản cập nhật đã được cài đặt nhưng hệ thống yêu cầu khởi

động lại (reboot) trước khi bản cập nhật này sẽ chạy. Do đó, cần rõ ràng rằng truy vấn nên thể hiện cả phiên bản được thực hiện gần đây nhất cũng như bản cập nhật được cài đặt gần đây nhất.

FPT_TUD_EXT.1.2 TSF phải cung cấp cho các *quản trị viên an toàn* khả năng tự khởi tạo các bản cập nhật cho phần mềm/phần sụn TOE một cách thủ công và [lựa chọn: *hỗ trợ tự kiểm tra các cập nhật, hỗ trợ các cập nhật tự động, không có cơ chế cập nhật khác*].

Chú thích áp dụng: Việc lựa chọn trong FPT_TUD_EXT.1.2 phân biệt sự hỗ trợ tự kiểm tra các cập nhật và hỗ trợ các cập nhật tự động. Tùy chọn đầu tiên đề cập đến một TOE kiểm tra xem có khả dụng một bản cập nhật mới hay không, thông báo cho quản trị viên (ví dụ, thông qua một tin nhắn trong phiên quản trị viên, thông qua tệp nhật ký) nhưng yêu cầu Quản trị viên đưa ra một số hành động để thực hiện cập nhật. Tùy chọn thứ hai đề cập đến một TOE kiểm tra các bản cập nhật và tự động cài đặt chúng khi có sẵn.

FPT_TUD_EXT.1.3 TSF phải cung cấp các phương tiện để xác thực bản cập nhật phần sụn/phần mềm cho TOE sử dụng [lựa chọn: *cơ chế chữ ký số, băm công khai*] trước khi cài đặt các bản cập nhật đó.

Chú thích áp dụng 1: Cơ chế chữ ký số được tham chiếu trong lựa chọn của FPT_TUD_EXT.1.3 là một trong những thuật toán được qui định trong FCS_COP.1(2). Hàm băm đã công bố được tham chiếu trong FPT_TUD_EXT.1.3 được tạo ra bởi một trong các hàm qui định trong FCS_COP.1(3). Tác giả ST phải lựa chọn cơ chế được thực hiện bởi TOE; có thể chấp thuận thực hiện cả hai cơ chế.

Chú thích áp dụng 2: Các phiên bản sau của tiêu chuẩn này sẽ yêu cầu sử dụng cơ chế chữ ký số cho các cập nhật tin cậy.

Chú thích áp dụng 3: Nếu các chứng thư được sử dụng trong cơ chế xác nhận cập nhật, các chứng thư được xác thực theo FIA_X509_EXT.1 và cần phải được lựa chọn từ FIA_X509_EXT.2.1. Ngoài ra, FPT_TUD_EXT.2 phải bao gồm trong ST.

Chú thích áp dụng 4: "Cập nhật" trong bối cảnh của SFR đề cập đến quá trình thay thế một thành phần phần mềm thường trú trên hệ thống, không khả biến bằng một phần mềm khác. Phần mềm cũ được gọi là hình ảnh NV, phần mềm sau là hình ảnh cập nhật. Mặc dù hình ảnh cập nhật thường mới hơn hình ảnh NV, tuy nhiên đây không phải là một yêu cầu bắt buộc. Có nhiều trường hợp hợp pháp chủ sở hữu hệ thống muốn chuyển một thành phần sang một phiên bản cũ hơn (ví dụ khi nhà sản xuất linh kiện phát hành bản cập nhật bị lỗi hoặc khi hệ thống dựa vào tính năng không còn có trong bản cập nhật). Tương tự như vậy, chủ sở hữu khác có thể muốn cập nhật với cùng một phiên bản với hình ảnh NV để phục hồi từ bộ nhớ bị lỗi.

Tất cả các thành phần phần mềm lẻ (ví dụ: ứng dụng, trình điều khiển, kernel, phần sụn) của TSF phải được ký số bởi nhà sản xuất tương ứng và sau đó được xác minh bởi cơ chế thực hiện cập nhật. Vì nó các thành phần được công nhận là có thể được ký bởi các nhà sản xuất khác nhau, nên quá trình cập nhật cần phải xác minh rằng cả bản cập nhật và bản hình ảnh NV đã được sản xuất bởi cùng một nhà

sản xuất (ví dụ bằng cách so sánh các khóa công khai) hoặc được ký bởi các khóa ký hợp pháp (ví dụ: xác minh thành công các chứng thư khi sử dụng các chứng thư X.509).

9.8.5 Các dấu thời gian (FPT_STM)

9.8.5.1 FPT_STM.1 Dấu thời gian đáng tin cậy

FPT_STM.1.1 TSF có thể cung cấp các dấu thời gian đáng tin cậy.

Chú thích áp dụng: TSF không cung cấp thông tin đáng tin cậy về thời gian hiện tại tại vị trí của TOE, nhưng tùy theo thông tin về thời gian và ngày bên ngoài, sẽ được cung cấp nhân công bởi quản trị viên hoặc thông qua việc sử dụng một máy chủ NTP. Thuật ngữ "dấu thời gian đáng tin cậy" đề cập đến việc sử dụng nghiêm ngặt thông tin về thời gian và ngày, được cung cấp bên ngoài, và ghi lại tất cả các thay đổi về cài đặt thời gian bao gồm thông tin về thời gian cũ và mới. Với thông tin này, thời gian thực cho tất cả các dữ liệu kiểm toán có thể tính toán được.

9.9 Truy cập TOE (FTA)

Điều này quy định cụ thể các yêu cầu liên quan đến an toàn của các phiên quản trị được thực hiện trên TOE. Đặc biệt, cả phiên cục bộ và từ xa đều được giám sát vì không hoạt động và bị khóa hoặc chấm dứt khi đạt tới một khoảng thời gian ngưỡng. Quản trị viên cũng phải có khả năng chấm dứt các phiên tương tác của mình, và phải có một thông báo tư vấn được hiển thị vào đầu mỗi phiên.

9.9.1 Khóa phiên được TSF khởi tạo (Extended – FTA_SSL_EXT)

9.9.1.1 FTA_SSL_EXT.1 Khóa phiên được TSF khởi tạo

FTA_SSL_EXT.1.1 TSF phải, đối với các phiên tương tác cục bộ, [lựa chọn:

- *Khóa phiên - vô hiệu hóa bất kỳ hoạt động nào của thiết bị truy cập / hiển thị dữ liệu người dùng ngoài việc mở khóa phiên và yêu cầu quản trị viên xác thực lại cho TSF trước khi mở khóa phiên;*
- *Kết thúc phiên]*

Sau một giai đoạn thời gian không hoạt động qui định bởi Quản trị viên.

9.9.2 Kết thúc và khóa phiên (FTA_SSL)

9.9.2.1 FTA_SSL.3 Kết thúc được khởi tạo bởi TSF

FTA_SSL.3.1 Sàng lọc: TSF phải kết thúc một phiên tương tác **từ xa** sau một khoảng thời gian không hoạt động phiên được Quản trị viên cấu hình.

9.9.2.2 FTA_SSL.4 Kết thúc được khởi tạo bởi người dùng

FTA_SSL.4.1 Sàng lọc: TSF phải cho phép kết thúc phiên tương tác của chính **Quản trị viên**

9.9.3 Các banner truy cập TOE (FTA_TAB)

9.9.3.1 FTA_TAB.1 Các banner truy cập TOE mặc định

FTA_TAB.1.1 Sàng lọc: *Trước khi thiết lập một phiên người dùng- quản trị viên,* TSF phải hiển thị thông báo tư vấn được quản trị viên an toàn chỉ định và thông báo cảnh báo về sự chấp thuận liên quan đến việc sử dụng TOE.

Chú thích áp dụng: Yêu cầu này được áp dụng cho các phiên tương tác giữa người dùng và TOE. Các đơn vị CNTT thiết lập các kết nối hoặc các kết nối có lập trình (ví dụ, các cuộc gọi thủ tục từ xa qua mạng) không bắt buộc phải có yêu cầu này.

9.10 Các kênh/đường dẫn tin cậy (FTP)

Để giải quyết các vấn đề liên quan đến truyền dữ liệu nhạy cảm đến và đi từ TOE, các TOE tuân thủ sẽ cung cấp mã hóa cho các đường dẫn truyền giữa chúng và điểm cuối. Các kênh này được thực hiện bằng cách sử dụng một (hoặc nhiều hơn) bốn giao thức chuẩn: IPsec, TLS, HTTPS, và SSH. Các giao thức này được quy định bởi RFC cung cấp đưa ra nhiều lựa chọn thực hiện. Các yêu cầu đã được áp dụng đối với một số các lựa chọn này (đặc biệt là các lựa chọn cho các nguyên mẫu mã hóa) để cung cấp khả năng tương tác và chống lại cuộc tấn công mã hóa.

Ngoài việc cung cấp bảo vệ chống lại tiết lộ (và phát hiện sửa đổi) cho các giao tiếp, mỗi giao thức được mô tả (IPsec, SSH, TLS và HTTPS) cung cấp xác thực hai chiều ở mỗi điểm cuối theo cách an toàn mã hóa, có nghĩa là ngay cả khi có một kẻ tấn công nguy hiểm giữa hai điểm cuối, thì bất kỳ nỗ lực để đại diện cho chính mình vào một trong hai điểm cuối của đường dẫn giao tiếp như bên giao tiếp khác sẽ được phát hiện.

9.10.1 Kênh tin cậy (FTP_ITC)

9.10.1.1 FTP_ITC.1 Kênh tin cậy Inter-TSF (đã được tinh chỉnh)

FTP_ITC.1.1 TSF phải có khả năng sử dụng [Lựa chọn: *IPsec, SSH, TLS, HTTPS*] để cung cấp một kênh thông tin kết nối đáng tin cậy giữa TSF và các thực thể IT được ủy quyền hỗ trợ các khả năng sau: server kiểm tra, [lựa chọn: *server xác thực, chỉ định: các khả năng khác*], có sự khác biệt về mặt logic với các kênh truyền thông khác và có khả năng xác định chắc chắn các điểm kết thúc và bảo vệ tính an toàn của dữ liệu kênh và phát hiện các trường hợp sửa đổi dữ liệu kênh.

FTP_ITC.1.2 TSF phải cho phép **TSF, hoặc các thực thể IT được ủy quyền** thực hiện hoạt động kết nối thông tin thông qua kênh đáng tin cậy.

FTP_ITC.1.3 TSF phải bắt đầu thực hiện hoạt động thông tin kết nối thông qua kênh đáng tin cậy [chỉ định: *danh sách các dịch vụ mà TSF có thể kết nối*].

Chú thích áp dụng: Mục đích của yêu cầu trên là cung cấp một phương tiện mà giao thức mã hóa có thể được sử dụng để bảo vệ thông tin kết nối bên ngoài với các thực thể IT được ủy quyền mà TOE tương tác để thực hiện các chức năng của nó. TOE sử dụng ít nhất một trong các giao thức được liệt kê để kết nối với máy chủ có tính năng thu thập thông tin kiểm toán. Nếu TOE kết nối với một máy chủ xác thực (ví dụ, RADIUS), thì tác giả ST chọn "máy chủ xác thực" trong FTP_ITC.1.1 và kết nối này

phải có khả năng được bảo vệ bởi một trong các giao thức được liệt kê. Nếu các thực thể IT được ủy quyền khác (ví dụ: máy chủ NTP) được bảo vệ, tác giả ST sẽ tiến hành các chỉ định phù hợp (cho các thực thể đó) và đưa ra các lựa chọn (đối với các giao thức được sử dụng để bảo vệ các kết nối đó). Tác giả ST chọn (các) cơ chế được hỗ trợ bởi TOE, và sau đó đảm bảo rằng các yêu cầu về giao thức chi tiết trong Phụ lục B tương ứng với lựa chọn của họ đã được đưa ra trong ST. Nếu TLS được chọn, tác giả ST sẽ yêu cầu FCS_TLSC_EXT.2 thay vì FCS_TLSC_EXT.1.

Mặc dù không có yêu cầu từ phía thực hiện kết nối, tuy nhiên, trong chỉ định cho FTP_ITC.1.3, tác giả ST đã liệt kê các dịch vụ mà TOE có thể bắt đầu tiến hành kết nối với thực thể CNTT được ủy quyền.

Yêu cầu này hàm ý rằng các thông tin kết nối không chỉ được bảo vệ khi chúng vừa được thiết lập mà còn được kết nối lại sau khi mất điện. Có thể xảy ra trường hợp một số phần cài đặt TOE tham gia thiết lập các đường hầm theo phương pháp thủ công để tự bảo vệ các kết nối khác, và nếu sau khi mất điện, TOE cố gắng thiết lập lại kết nối một cách tự động (khi cần thiết) với can thiệp bằng phương pháp thủ công, có thể có một cửa sổ tạo ra, tại đây đối tượng tấn công có thể có được thông tin quan trọng hoặc được chấp thuận kết nối.

9.10.2 Đường dẫn đáng tin cậy (FTP_TRP)

9.10.2.1 FTP_TRP.1 Đường dẫn đáng tin cậy (đã được tinh chỉnh)

FTP_TRP.1.1 TSF phải có khả năng sử dụng [Lựa chọn: ***IPsec, SSH, TLS, HTTPS***] để cung cấp một kênh thông tin kết nối đáng tin cậy giữa TSF và các **quản trị viên từ xa** được ủy quyền có sự khác biệt về logic với các đường dẫn khác và có khả năng xác định chắc chắn các điểm kết thúc đồng thời *bảo vệ tính an toàn của dữ liệu kênh và phát hiện các trường hợp sửa đổi dữ liệu kênh.*

FTP_TRP.1.2 TSF cho phép các **quản trị viên từ xa** thực hiện thông tin kết nối thông qua đường dẫn đáng tin cậy.

FTP_TRP.1.3 TSF yêu cầu sử dụng đường dẫn đáng tin cậy để **xác thực quản trị viên ban đầu và tất cả hoạt động quản trị từ xa.**

Chú thích áp dụng: Yêu cầu này đảm bảo các quản trị viên từ xa được ủy quyền có thể thực hiện kết nối với TOE thông qua một đường dẫn đáng tin cậy và tất cả các kết nối với TOE thông qua các quản trị viên từ xa được thực hiện thông qua đường dẫn này. Dữ liệu được truyền trong kênh truyền tin đáng tin cậy này được mã hóa theo quy định của giao thức được chọn trong lựa chọn đầu tiên. Tác giả ST chọn (các) cơ chế được hỗ trợ bởi TOE, và sau đó đảm bảo rằng các yêu cầu về giao thức chi tiết trong Phụ lục B tương ứng với lựa chọn giao thức được đưa vào trong ST.

9.11 Tường lửa (FFW)

9.11.1 Tường lửa lọc lưu lượng có trạng thái (FFW_RUL_EXT)

Để giải quyết các vấn đề liên quan đến việc tiết lộ trái phép thông tin, truy cập không hợp lệ vào các dịch vụ, lạm dụng dịch vụ, gián đoạn hoặc từ chối dịch vụ, và thăm dò dựa trên mạng lưới hệ thống, TOE tuân thủ sẽ thực hiện khả năng Lọc lưu lượng có trạng thái. Khả năng này sẽ hạn chế luồng lưu

lượng mạng giữa các mạng được bảo vệ và các mạng kết nối khác dựa theo địa chỉ mạng và các cổng của nút mạng xuất phát (nguồn) và/hoặc nhận (đích) lưu lượng truy cập mạng cũng như thông tin kết nối đã được thiết lập.

Hoạt động kiểm tra gói tin có trạng thái được sử dụng để hỗ trợ thực hiện lưu lượng gói tin thông qua TOE. Thay vì áp dụng bộ quy tắc đối với từng gói tin được xử lý tại một giao diện TOE, TOE sẽ xác định xem gói tin có thuộc kết nối đã được thiết lập và được "phê duyệt" hay không. Một bộ thuộc tính tối thiểu được sử dụng để xác định liệu một gói tin có phải là một phần của phiên đã được thiết lập cho TCP và UDP và tác giả ST được phép mở rộng các thuộc tính đã được xem xét cho các phiên TCP và bổ sung giao thức ICMP nếu muốn.

Các TOE tuân thủ sẽ thực hiện khả năng ghi lưu lượng mạng. Cụ thể, TOE sẽ cung cấp phương tiện để quản trị viên lập cấu hình các quy tắc tường lửa cụ thể nhằm thực hiện chức năng "ghi" khi lưu lượng mạng được xác định là phù hợp với quy tắc đã được cấu hình. Do đó, bất cứ khi nào quy tắc của tường lửa được cấu hình khớp với "log" sẽ trả về bản ghi sự kiện.

9.11.1.1 FFW_RUL_EXT.1 Lọc lưu lượng có trạng thái

FFW_RUL_EXT.1.1 TSF phải thực hiện việc kiểm toán lưu lượng truy cập trên thanh trạng thái của các mạng gói tin để xử lý TOE.

Chú thích áp dụng: Tính năng này xác định chính sách (Lọc lưu lượng có trạng thái) được áp dụng cho các gói tin mạng được xử lý tại các giao diện của TOE. Mỗi gói tin nhận được ở một giao diện của TOE có một bộ quy tắc thể hiện việc áp dụng chính sách này, hoặc sẽ được xác định rằng gói tin thuộc về một kết nối đã được thiết lập. Các phần tử còn lại trong thành phần này cung cấp thông tin chi tiết về chính sách này.

Yêu cầu này sẽ được thực thi ngay cả khi lưu lượng mạng của giao diện mạng bị bão hòa/quá tải.

Điểm quan trọng cần lưu ý là TOE, vốn bao gồm cả nền tảng cơ bản, không thể cho phép các gói tin mạng lưu thông trừ khi trong bộ quy tắc có quy tắc cho phép lưu thông, hoặc gói tin được coi là thuộc một kết nối đã được thiết lập và cho phép lưu thông. Nguyên tắc này cần phải được tuân thủ triệt để khi khởi động TOE, và khi TOE gặp lỗi.

FFW_RUL_EXT.1.2 TSF phải cho phép xác định các quy tắc Lọc lưu lượng có trạng thái, sử dụng các trường giao thức mạng sau:

- ICMPv4
    - Loại
    - Mã
- ICMPv6
    - Loại

- Mã

- IPv4
  - Địa chỉ nguồn
  - Địa chỉ đích
  - Giao thức tầng giao vận
- IPv6
  - Địa chỉ nguồn
  - Địa chỉ đích
  - Giao thức tầng giao vận
  - [lựa chọn: *loại mào đầu IPv6 mở rộng [chỉ định: danh sách các trường trong mào đầu mở rộng IPv6], không có trường khác*]
- TCP
  - Cổng nguồn
  - Cổng đích
- UDP
  - Cổng nguồn
  - Cổng đích
- Và giao diện riêng biệt.

Chú thích áp dụng: Tính năng này xác định các thuộc tính khác nhau có thể áp dụng khi xây dựng các quy tắc sẽ được thực thi theo yêu cầu này - giao diện áp dụng là một thuộc tính của TOE và các thuộc tính còn lại được xác định trong các RFC liên quan. Lưu ý rằng 'Giao thức tầng giao vận" là trường IPv4 / IPv6 xác định giao thức áp dụng, chẳng hạn như TCP, UDP, ICMP hoặc GRE. Các mào đầu mở rộng IPv6 được định nghĩa trong RFC 2460 và tác giả ST có thể xác định các trường nằm trong mỗi mào đầu mở rộng được hỗ trợ, nếu có thể sử dụng làm thuộc tính xây dựng quy tắc kiểm tra. Ngoài ra, 'Giao diện' được nêu ở trên là cổng bên ngoài nơi truyền hoặc nhận lưu lượng mạng thích hợp.

FFW_RUL_EXT.1.3 TSF phải cho phép kết nối các hoạt động sau với các quy tắc Lọc lưu lượng mạng có trạng thái: cho phép hoặc hủy khả năng đăng nhập hoạt động.

Chú thích áp dụng: Tính năng này xác định các hoạt động có thể liên kết với các quy tắc được sử dụng để khớp lưu lượng mạng. Lưu ý rằng dữ liệu cần đăng nhập được xác định trong các yêu cầu Kiểm toán an toàn trong Bảng 1.

FFW_RUL_EXT.1.4 TSF phải cho phép các quy tắc Lọc lưu lượng mạng có trạng thái gắn với từng giao diện mạng riêng biệt.

Chú thích áp dụng: Tính năng này xác định vị trí gán các quy tắc. Cụ thể, một TOE phù hợp phải có khả năng gán các quy tắc lọc cho mỗi giao diện mạng riêng biệt và có sẵn mà xử lý lưu lượng mạng tầng 3 và 4. Một giao diện mạng riêng biệt có thể là giao diện vật lý hoặc logic tuy nhiên không bắt buộc phải nhìn thấy được từ góc độ mạng (ví dụ: không cần phải gán địa chỉ IP cho nó).

Lưu ý rằng có thể có một bộ quy tắc riêng cho mỗi giao diện hoặc có một bộ giao thức chia sẻ mà liên kết các quy tắc với các giao diện cụ thể theo một cách nào đó.

FFW_RUL_EXT.1.5 TSF phải:

a) chấp nhận gói tin mạng mà không cần xử lý thêm các quy tắc Lọc lưu lượng có trạng thái nếu nó khớp với phiên được thiết lập và được cho phép đối với các giao thức sau: TCP, UDP, [lựa chọn: ICMP, *không có giao thức khác*] dựa trên các thuộc tính gói mạng sau:

1. TCP: địa chỉ nguồn và đích, cổng nguồn và đích, số thứ tự, cờ;
2. UDP: địa chỉ nguồn và đích, cổng nguồn và đích;
3. [lựa chọn: *'ICMP: địa chỉ nguồn và đích, loại, [lựa chọn: mã, [chỉ định: danh sách các thuộc tính phù hợp]]', không có giao thức khác*].

b) Loại bỏ các lưu lượng truy cập hiện có ra khỏi bộ lưu lượng truy cập đã thiết lập dựa trên: [lựa chọn: *thời gian chờ không hoạt động phiên, hoàn thành lưu lượng thông tin dự kiến*].

Chú thích áp dụng: Tính năng này yêu cầu phải xác định các giao thức mà TOE có thể xác định và quản lý trạng thái sao cho có thể thiết lập và sử dụng các phiên để đưa ra quyết định lưu lượng truy cập trái ngược với việc xử lý đầy đủ các quy tắc được định cấu hình. Tính năng này cũng yêu cầu sử dụng các thuộc tính thích hợp để xác định liệu một gói mạng có tương thích hay không và phiên thiết lập có được xác định hay không.

Nếu ICMP được chọn là một giao thức, các địa chỉ nguồn và đích cần phải được xem xét để xác định xem gói tin có thuộc một kết nối đã được thiết lập hay không. Loại và thuộc tính mã có thể được sử dụng để tạo ra tính năng hiệu quả hơn trong việc xác định xem liệu một gói tin ICMP có phải là những gì được mong đợi trong luồng kết nối được thiết lập. Ví dụ, người ta không mong đợi lời đáp echo sẽ là một phần trong lưu lượng thông tin nếu một yêu cầu echo đã không được tiếp nhận. Chỉ định mở trong việc lựa chọn các thuộc tính ICMP được sử dụng cho các trường hợp thực thi có thể sử dụng thuộc tính IPv6.

Mục b) thuộc phần này yêu cầu đặc tả cách thức tường lửa có thể xác định rằng các luồng thông tin đã được thiết lập nên được loại bỏ khỏi tập hợp các luồng thông tin đã được thiết lập bằng cách quan sát các sự kiện chẳng hạn như sự kiện chấm dứt của một phiên TCP được khởi tạo bởi một trong hai điểm đầu cuối có cờ FIN trong gói tin TCP. Nếu các giao thức được xử lý theo cách khác nhau, người ta hy vọng rằng ST sẽ xác định các khác biệt này.

FFW_RUL_EXT.1.6 TSF phải thực thi các quy tắc Lọc lưu lượng có trạng thái trên tất cả lưu lượng mạng, cụ thể như dưới đây:

a) TSF sẽ loại bỏ và có khả năng [lựa chọn: *đếm, ghi lại*] các gói dữ liệu không hợp lệ;

b) TSF sẽ loại bỏ và có khả năng [lựa chọn: *đếm, ghi lại*] các gói tin bị phân mảnh mà không thể lắp ghép lại một cách hoàn chỉnh;

c) TSF sẽ loại bỏ và có khả năng ghi lại các gói dữ liệu có địa chỉ nguồn được xác định đang nằm trong một mạng mạng quảng bá;

d) TSF sẽ loại bỏ và có khả năng ghi các gói tin có địa chỉ nguồn của được xác định nằm trong mạng multicast; mức độ TSF sẽ loại bỏ và có khả năng ghi lại các gói tin mạng có địa chỉ nguồn được xác định là địa chỉ loopback;

e) TSF sẽ loại bỏ và có khả năng ghi lại các gói tin mạng có địa chỉ nguồn hoặc địa chỉ đích không xác định (tức là 0.0.0.0) hoặc một địa chỉ "dành cho việc sử dụng trong tương lai" (ví dụ: 240.0.0.0/4) theo quy định tại RFC 5735 cho IPv4;

f) TSF sẽ loại bỏ và có khả năng ghi lại các gói tin mạng có địa chỉ nguồn hoặc địa chỉ đích được xác định là "địa chỉ không xác định" hoặc địa chỉ "dành cho việc xác định và sử dụng trong tương lai" (ví dụ các địa chỉ máy trạm không có trong phạm vi địa chỉ này: 2000::/3) theo quy định tại RFC 3513 đối với IPv6;

g) TSF sẽ loại bỏ và có khả năng ghi lại các gói tin mạng với các tùy chọn IP: Định tuyến nguồn thiếu chặt chẽ, Định tuyến nguồn chính xác hoặc Định tuyến cụ thể cần ghi nhận; và

h) [lựa chọn: *[chỉ định: các quy tắc mặc định khác thực thi bởi TOE], không có quy tắc nào khác*].

Chú thích áp dụng: Các sửa đổi trong tương lai của tiêu chuẩn này sẽ yêu cầu TOE thực hiện các quy tắc mặc định này mà không cần áp dụng cấu hình.

FFW_RUL_EXT.1.7 TSF phải có khả năng loại bỏ và ghi lại các quy tắc sau:

a) TSF sẽ loại bỏ và có khả năng ghi lại các gói tin mạng có địa chỉ nguồn là địa chỉ của giao diện mạng nơi tiếp nhận gói tin mạng;

b) TSF sẽ loại bỏ và có khả năng ghi lại các gói tin mạng có địa chỉ nguồn hoặc địa chỉ đích là địa chỉ liên kết cục bộ;

c) TSF sẽ loại bỏ và có khả năng ghi lại các gói tin mạng có địa chỉ nguồn không thuộc các mạng có kết nối với giao diện mạng mà gói tin mạng đã nhận.

Chú thích áp dụng: Lưu ý rằng các quy tắc này có thể được lập cấu hình.

FFW_RUL_EXT.1.8, TSF phải xử lý các quy tắc lọc lưu lượng truy cập áp dụng theo trình tự xác định được kiểm soát.

Chú thích áp dụng: Tính năng này yêu cầu quản trị viên phải có khả năng xác định trình tự xử lý các quy tắc lọc được cấu hình cho phù hợp. Quy tắc lọc chỉ áp dụng khi một phiên cho phép chưa được thiết lập hoặc quy tắc động đã được tạo lập.

FFW_RUL_EXT.1.9 The TSF phải từ chối luồng gói tin nếu quy tắc không khớp.

Chú thích áp dụng: Tính năng này yêu cầu rằng, trừ khi một gói tin là một phần của một phiên được thiết lập, hành vi luôn từ chối lưu lượng truy cập mạng khi không có quy tắc áp dụng và không yêu cầu có các hoạt động khác, mặc dù chúng không nhất thiết bị cấm.

FFW_RUL_EXT.1.10 TSF có khả năng giới hạn một số kết nối TCP half-open được xác định ở khía cạnh quản trị. Trường hợp đạt tới giới hạn cấu hình, các kết nối mới sẽ bị bỏ và trường hợp bỏ sẽ được [lựa chọn: *đếm, ghi lại*].

Chú thích áp dụng: Kết nối TCP half-open là một dạng kết nối chưa hoàn thiện đầy đủ quá trình bắt tay ba bước như đã nêu trong RFC 793. Các kết nối TCP chưa hoàn thiện, ví dụ các kết nối mới hoàn thành các phần SYN và SYN-ACK của quá trình bắt tay ba bước, sẽ sử dụng các tài nguyên trong các máy chủ cuối và các thiết bị Lọc lưu lượng có trạng thái trong đường truyền lưu lượng và, khi đủ số lượng, có thể dẫn đến tình trạng từ chối dịch vụ. Để bảo vệ chính TOE và các dịch vụ bảo vệ theo mục tiêu đặt ra, các TOE phù hợp sẽ có khả năng hạn chế số lượng các kết nối TCP nửa mở.

10 Yêu cầu đảm bảo an toàn

Tiêu chuẩn này xác định các yêu cầu đảm bảo an toàn (SAR) để đánh giá viên áp dụng đánh giá tài liệu hướng dẫn phục vụ cho việc đánh giá và thực hiện kiểm tra độc lập.

Điều này liệt kê bộ SAR trong TCVN 8709-3:2011 đã được yêu cầu trong các đánh giá đối với tiêu chuẩn này. Các hoạt động đánh giá cá nhân cần được thực hiện đã được nêu tại [SD].

Mô hình chung để đánh giá TOE theo các ST được viết để tuân thủ tiêu chuẩn này được mô tả như sau: Sau khi ST đã được phê duyệt để đánh giá, phòng thử nghiệm sẽ nhận TOE, môi trường hỗ trợ thử nghiệm (nếu cần) và tài liệu hướng dẫn cho TOE. Phòng thử nghiệm sẽ thực hiện các hoạt động đánh giá theo Phương pháp đánh giá an toàn công nghệ thông tin [CEM] cho các yêu cầu đảm bảo an toàn thông tin ASE và ALC. Phòng thử nghiệm cũng thực hiện các hoạt động đánh giá có trong SD, nhằm mục đích giải thích các yêu cầu đảm bảo đánh giá an toàn thông tin CEM khác khi chúng áp dụng đối với công nghệ cụ thể nêu trong TOE. Các hoạt động đánh giá được ghi trong SD cũng giải thích rõ những gì mà nhà thiết kế cần để chứng minh TOE phù hợp với PP này.

Các yêu cầu đảm bảo an toàn TOE được xác định trong Bảng 2.

Bảng 2 - Các yêu cầu đảm bảo an toàn

Lớp bảo đảm an toàn	Thành phần đảm bảo an toàn
Mục tiêu an toàn (ASE)	Các tuyên bố tuân thủ (ASE_CCL.1)
	Định nghĩa thành phần mở rộng (ASE_ECD.1)
	Giới thiệu ST (ASE_INT.1)
	Các mục tiêu an toàn cho môi trường vận hành
	Các yêu cầu an toàn (ASE_REQ.1)
	Định nghĩa vấn đề an toàn (ASE_SPD.1)
	Đặc tả tóm tắt TOE (ASE_TSS.1)
Phát triển (ADV)	Đặc tả chức năng cơ bản (ADV_FSP.1)
Tài liệu hướng dẫn (AGD)	Hướng dẫn sử dụng (AGD_OPE.1)
	Thủ tục chuẩn bị (AGD_PRE.1)
Hỗ trợ vòng đời (ALC)	Gán nhãn cho TOE (ALC_CMC.1)
	Phạm vi CM TOE (ALC_CMS.1)
Thử nghiệm (ATE)	Thử nghiệm độc lập – mẫu thử nghiệm (ATE_IND.1)
Đánh giá điểm yếu (AVA)	Khảo sát điểm yếu (AVA_VAN.1)

10.1 ASE: Mục tiêu an toàn

ST được đánh giá theo các hoạt động ASE chỉ định trong CEM. Ngoài ra, có thể có các hoạt động đánh giá được chỉ định trong SD để đưa các mô tả cần thiết vào trong TSS, với nội dung cụ thể đối với từng loại công nghệ TOE.

Phụ lục D mô tả các thông tin dự kiến sẽ được cung cấp liên quan đến chất lượng của entropy trong bộ sinh bit ngẫu nhiên.

ASE_TSS.1.1C Sàng lọc: Phần đặc tả tóm tắt TOE sẽ mô tả cách thức TOE đáp ứng mỗi SFR. **Trong trường hợp phân tích entropy, TSS được kết hợp sử dụng cùng, bao gồm các thông tin bổ sung cần thiết về Entropy**.

Các yêu cầu đặt ra đối với việc tuân thủ chính xác Đích an toàn (ST) được mô tả trong điều 6 và trong [SD-ND, 3.1].

10.2 ADV: Phát triển

Thông tin thiết kế về TOE có trong tài liệu hướng dẫn, có sẵn cho người dùng cuối, kèm theo phần TSS của ST và bất kỳ thông tin bổ sung cần thiết không được thực hiện công khai theo yêu cầu của tiêu chuẩn này.

10.2.1 Đặc tả chức năng cơ bản (ADV_FSP.1)

Phần đặc tả chức năng này mô tả các giao diện chức năng an toàn TOE (TSFI). Không cần phải có một đặc tả chính thức hoặc đầy đủ về các giao thức này. Ngoài ra, do các TOE phù hợp với tiêu chuẩn này nhất thiết phải có các giao diện với môi trường hoạt động mà người sử dụng TOE không trực tiếp sử dụng nên cần có ít điểm chỉ rõ về các giao diện này bởi lẽ chỉ có thể thực hiện thử nghiệm gián tiếp

các giao diện như vậy. Đối với tiêu chuẩn này, các hoạt động đánh giá cho họ này tập trung vào khả năng hiểu các giao diện được trình bày trong TSS để đáp ứng các yêu cầu chức năng và các giao diện được trình bày trong tài liệu AGD. Không cần thêm bất kỳ tài liệu "đặc tả chức năng" nào khác sử dụng cho hoạt động đánh giá xác định trong SD.

Các hoạt động đánh giá trong SD gắn liền với các SFR áp dụng; vì các hoạt động này có gắn kết trực tiếp với các SFR nên việc dò tìm trong thành phần ADV_FSP.1.2D đã được thực hiện triệt để và không cần tài liệu bổ sung.

10.3 AGD: Tài liệu hướng dẫn

Tài liệu hướng dẫn sẽ được cung cấp kèm theo ST. Tài liệu này cần có nội dung mô tả cách thức nhân viên IT xác minh rằng môi trường hoạt động có thể hoàn thành vai trò của nó đối với chức năng an toàn. Tài liệu hướng dẫn nên được trình bày đơn giản để nhân viên IT có thể đọc hiểu dễ dàng.

Tài liệu hướng dẫn phải được cung cấp cho tất cả môi trường hoạt động được sản phẩm hỗ trợ như đã ghi trong ST. Tài liệu này bao gồm:

- Các hướng dẫn để cài đặt thành công TSF trong môi trường đó; và

- Các hướng dẫn để quản lý an toàn TSF như là một sản phẩm và như là một thành phần của môi trường hoạt động lớn hơn; và

- Các hướng dẫn về việc cung cấp khả năng quản trị được bảo vệ.

Ngoài ra, cần cung cấp các tài liệu hướng dẫn liên quan đến chức năng an toàn cụ thể; các yêu cầu đối với tài liệu hướng dẫn này được trình bày trong các hoạt động đánh giá tại SD.

10.3.1 Tài liệu hướng dẫn sử dụng (AGD_OPE.1)

Không có tài liệu hướng dẫn sử dụng riêng. Các nội dung hướng dẫn cho người dùng, quản trị viên và nhà phát triển ứng dụng có thể được trình bày xen kẽ ở các tài liệu hoặc các trang web.

Nhà phát triển ứng dụng nên xem xét các hoạt động đánh giá có trong SD để xác định nội dung chi tiết của tài liệu hướng dẫn sẽ được đánh giá viên kiểm tra sau này. Điều này giúp cung cấp các thông tin cần thiết cho việc chuẩn bị tài liệu hướng dẫn đạt yêu cầu.

10.3.2 Quy trình chuẩn bị (AGD_PRE.1)

Ngoài tài liệu hướng dẫn hoạt động, nhà phát triển ứng dụng cần xem xét các hoạt động đánh giá để xác định nội dung yêu cầu đặt ra đối với quy trình chuẩn bị.

10.4 Lớp ALC: Hỗ trợ vòng đời

Ở mức độ đảm bảo cung cấp cho các TOE phù hợp với tiêu chuẩn này, hỗ trợ vòng đời được giới hạn ở các khía cạnh vòng đời mà người dùng cuối có thể theo dõi, hoàn toàn không liên quan đến hoạt động kiểm tra quy trình phát triển và quản lý cấu hình của nhà cung cấp TOE. Điều này không có nghĩa

sẽ giảm bớt vai trò hoạt động quan trọng của nhà phát triển ứng dụng trong việc đóng góp vào độ tin cậy chung của một sản phẩm; Thay vào đó, điều này phản ánh các thông tin cần được cung cấp cho hoạt động đánh giá ở mức độ đảm bảo này.

10.4.1 Ghi nhãn TOE (ALC_CMC.1)

Tính năng này được dùng để xác định TOE sao cho nó có thể phân biệt được với các sản phẩm hoặc phiên bản khác từ cùng một nhà cung cấp và có thể dễ dàng xác định khi được mua bởi người dùng cuối. Nhãn có thể bao gồm "nhãn cứng" (ví dụ, đóng dấu vào phần kim loại, nhãn giấy) hoặc "nhãn mềm" (ví dụ, trình bày bằng điện tử khi được yêu cầu).

Đánh giá viên thực hiện các đơn vị công việc CEM liên quan đến ALC_CMC.1.

10.4.2 Phạm vi TOE CM (ALC_CMS.1)

Xét trong phạm vi TOE và các yêu cầu về bằng chứng đánh giá liên quan, đánh giá viên thực hiện các đơn vị công việc CEM liên quan đến ALC_CMS.1.

10.5 Lớp ATE: Thử nghiệm

Thử nghiệm là cụ thể theo khía cạnh chức năng của hệ thống cũng như khía cạnh theo thiết kế hoặc các điểm yếu thực thi. Các thử nghiệm trước được thực hiện thông qua họ ATE_IND và thử nghiệm sau được thực hiện thông qua họ AVA_VAN. Đối với tiêu chuẩn này, thử nghiệm được thực hiện dựa trên các chức năng và giao diện được quảng cáo và phụ thuộc vào tính sẵn có của thông tin thiết kế. Một trong những đầu ra chính của quá trình đánh giá là báo cáo thử nghiệm như đã nêu trong các yêu cầu sau.

10.5.1 Thử nghiệm độc lập – Tính tuân thủ (ATE_IND.1)

Thử nghiệm được thực hiện để xác nhận chức năng được mô tả trong TSS cũng như tài liệu hướng dẫn (bao gồm các hướng dẫn "cấu hình được đánh giá"). Trọng tâm của thử nghiệm là để xác nhận rằng các yêu cầu được nêu trong điều 9 được đáp ứng. Các hoạt động đánh giá trong SD xác định các hoạt động thử nghiệm cụ thể cần thiết để xác minh sự phù hợp với các SFR. Đánh giá viên xây dựng một báo cáo thử nghiệm ghi lại kế hoạch và kết quả thử nghiệm cũng như các lập luận bao trùm tập trung vào các tổ hợp nền tảng/TOE đang tuyên bố tuân thủ với tiêu chuẩn này.

10.6 Lớp AVA: Đánh giá điểm yếu

Đối với phiên bản đầu tiên của tiêu chuẩn này, dự kiến sẽ khảo sát các nguồn mở để phát hiện các điểm yếu đã từng được phát hiện trong các loại sản phẩm này và đưa nội dung này vào thảo luận AVA_VAN. Trong hầu hết các trường hợp, các điểm yếu này đòi hỏi phức tạp hơn các điểm yếu của một đối tượng tấn công thông thường. Thông tin này sẽ được sử dụng để thiết lập các hồ sơ bảo vệ trong tương lai.

10.6.1 Khảo sát điểm yếu (AVA_VAN.1)

Phụ lục A trong [SD] đưa ra hướng dẫn để đánh giá viên thực hiện phân tích điểm yếu.

Phụ lục A
(Quy định)
Các yêu cầu tùy chọn

A.0 Giới thiệu

Như đã nêu trong phần giới thiệu về tiêu chuẩn này, các yêu cầu cơ bản (những gì phải được thực hiện bởi TOE) được chứa trong phần thân của tiêu chuẩn này. Ngoài ra, còn có hai loại yêu cầu khác được quy định trong Phụ lục A và B.

Loại đầu tiên (trong Phụ lục này) bao gồm các yêu cầu có thể được đưa vào ST, nhưng không bắt buộc để TOE xác nhận sự phù hợp với tiêu chuẩn này. Loại thứ hai (trong Phụ lục B) bao gồm các yêu cầu dựa trên các lựa chọn trong các SFR khác từ PP: nếu lựa chọn nhất định được thực hiện, thì các yêu cầu bổ sung trong phụ lục đó sẽ cần phải được bao gồm trong phần thân của ST (ví dụ, các giao thức mật mã được chọn trong một yêu cầu kênh đáng tin cậy).

A.1. Kiểm toán các sự kiện cho các SFR tùy chọn

Bảng 3 - SFR tùy chọn TOE và các sự kiện có thể kiểm toán

Yêu cầu	Các sự kiện có thể kiểm toán	Các nội dung ghi chép kiểm toán bổ sung
FAU_STG.1	Không.	Không.
FAU_STG_EXT.2	Không.	Không.
FAU_STG_EXT.3	Cảnh báo về thiếu không gian lưu trữ cho các sự kiện kiểm toán.	Không.
FMT_MOF.1(1)/Audit	Sửa đổi hành vi truyền dữ liệu kiểm toán tới một thực thể CNTT bên ngoài.	Không.
FMT_MOF.1(2)/Audit	Sửa đổi hành vi xử lý dữ liệu kiểm toán.	Không.
FMT_MOF.1(1)/AdminAct	Sửa đổi hành vi của TSF.	Không.
FMT_MOF.1(2)/AdminAct	Khởi động và ngừng các dịch vụ.	Không.

FMT_MOF.1(1)/LocSpace	Sửa đổi hành vi của chức năng kiểm toán khi không gian lưu trữ kiểm toán cục bộ đầy.	Không.
FMT_MTD.1/AdminAct	Sửa đổi, xóa, tạo/nhập các khóa mật mã.	Không.
FPT_FLS.1/LocalAudit Storage Space Full	Không.	Không.
FFW_RUL_EXT.2	Được định nghĩa trong ST.	Được định nghĩa trong ST.

A.2 Kiểm toán an toàn (FAU)

A.2.1 Kiểm toán an toàn lưu trữ sự kiện (FAU_STG.1 & Mở rộng – FAU_STG_EXT)

Không gian lưu trữ cục bộ cho dữ liệu kiểm toán có thể cần thiết với TOE, và TOE sau đó có thể yêu cầu bảo vệ dấu vết kiểm toán khỏi các sửa đổi không hợp pháp (bao gồm cả việc xóa bỏ) như đã mô tả tại FAU_STG.1. Không gian lưu trữ cục bộ cho dữ liệu kiểm toán của một thiết bị mạng là hữu hạn, và nếu không gian lưu trữ cục bộ bị vượt quá thì dữ liệu kiểm toán có thể bị mất. Quản trị viên phải quan tâm đến số lượng bản ghi kiểm toán bị mất, bị ghi đè... Con số này có thể là dấu hiệu cho thấy một vấn đề nghiêm trọng đã xảy ra sau khi không gian lưu trữ vượt quá dữ liệu kiểm toán được tạo liên tục. Do đó FAU_STG_EXT.2 và FAU_STG_EXT.3 được định nghĩa để thể hiện những khả năng tùy chọn này của thiết bị mạng.

A.2.1.1 FAU_STG.1 Bảo vệ lưu trữ bằng chứng kiểm toán

FAU_STG.1.1 TSF phải bảo vệ các hồ sơ kiểm toán được lưu trữ trong quá trình kiểm toán khỏi việc xóa trái phép.

FAU_STG.1.2 TSF phải có thể ngăn ngừa các sửa đổi trái phép vào các hồ sơ kiểm toán được lưu trữ trong dấu vết kiểm toán.

A.2.1.2 FAU_ STG_EXT.2 Tính toán dữ liệu kiểm toán bị mất

FAU_STG_EXT.2.1 TSF phải cung cấp thông tin về số lượng hồ sơ kiểm toán [lựa chọn: *bị xóa, ghi đè, chỉ định: các thông tin khác*] trong trường hợp lưu trữ cục bộ đã đầy và TSF thực hiện một trong các hành động được xác định trong FAU_STG_EXT.1.3.

Chú thích áp dụng: Tùy chọn này nên được chọn nếu TOE hỗ trợ chức năng này.

Trong trường hợp lưu trữ cục bộ cho các hồ sơ kiểm toán bị xóa bởi quản trị viên, các tính toán liên quan đến lựa chọn trong SFR nên được đặt lại về giá trị ban đầu (thường là 0). Tài liệu hướng dẫn nên chứa một cảnh báo cho quản trị viên về việc mất dữ liệu kiểm toán khi anh ta xóa lưu trữ cục bộ cho các hồ sơ kiểm toán.

A.2.1.3 FAU_ STG_EXT.3 Hiển thị cảnh báo cho không gian lưu trữ cục bộ

FAU_STG_EXT.3.1 TSF phải tạo ra một cảnh báo để thông báo cho người dùng trước khi không gian lưu trữ cục bộ cho dữ liệu kiểm toán được sử dụng tới hạn và/hoặc TOE sẽ mất dữ liệu kiểm toán do không gian cục bộ không đầy đủ.

Chú thích áp dụng: Tùy chọn này nên được chọn nếu TOE tạo ra như là cảnh báo để thông báo cho người dùng trước khi không gian lưu trữ cục bộ cho dữ liệu kiểm toán được sử dụng hết. Điều này có thể hữu ích nếu các sự kiện kiểm toán chỉ được lưu trữ trên không gian lưu trữ cục bộ.

Phải đảm bảo rằng thông điệp cảnh báo theo yêu cầu của FAU_STG_EXT.1.3 có thể được truyền đạt tới người dùng. Việc truyền thông phải được thực hiện thông qua bản ghi kiểm toán chính nó bởi vì nó không thể được đảm bảo rằng một phiên quản trị đang hoạt động tại thời điểm xảy ra sự kiện.

A.3 Quản lý an toàn (FMT)

A.3.1 Quản lý các chức năng trong TSF (FMT_MOF)

A.3.1.1 FMT_MOF.1 Quản lý hành vi chức năng an toàn

FMT_MOF.1.1(1)/Audit TSF phải hạn chế khả năng xác định hành vi, sửa đổi hành vi của các chức năng truyền dữ liệu kiểm toán tới một thực thể CNTT bên ngoài cho các quản trị viên an toàn.

Chú thích áp dụng: FMT_MOF.1(1)/Audit nên luôn được chọn nếu các giao thức truyền dẫn để truyền dữ liệu kiểm toán cho một thực thể CNTT bên ngoài như được định nghĩa trong FAU_STG_EXT.1.1 được cấu hình.

FMT_MOF.1.1(2)/Audit TSF phải hạn chế khả năng xác định hành vi, sửa đổi hành vi của các chức năng xử lý dữ liệu kiểm toán cho các quản trị viên an toàn.

Chú thích áp dụng: FMT_MOF.1(2)/Audit chỉ nên được chọn nếu xử lý dữ liệu kiểm toán được cấu hình. Thuật ngữ "xử lý dữ liệu kiểm toán" đề cập đến các tùy chọn khác nhau để lựa chọn và chỉ định trong các SFR FAU_STG_EXT.1.2, FAU_STG_EXT.1.3 và FAU_STG_EXT.2.

FMT_MOF.1.1(1)/AdminAct TSF phải hạn chế *khả năng sửa đổi hành vi* của các chức năng *TSF cho các quản trị viên an toàn.*

Chú thích áp dụng: FMT_MOF.1(1)/AdminAct chỉ nên được chọn nếu hành vi của các chức năng an toàn TOE được cấu hình.

FMT_MOF.1.1(2)/AdminAct TSF phải hạn chế khả năng cho phép, vô hiệu hóa các dịch vụ chức năng cho quản trị viên an toàn.

Chú thích áp dụng: FMT_MOF.1(2)/AdminAct chỉ nên chọn lựa quản trị viên có khả năng khởi động và tắt các dịch vụ.

FMT_MOF.1.1/LocSpace TSF phải hạn chế khả năng *xác định hành vi, sửa đổi hành vi* của các chức năng *kiểm toán chức năng* khi không gian lưu trữ kiểm toán cục bộ đầy cho các quản trị viên an toàn.

Chú thích áp dụng: FMT_MOF.1/LocSpace chỉ nên được chọn nếu hành vi của các chức năng kiểm toán khi không gian lưu trữ kiểm toán cục bộ đầy là cấu hình được.

A.3.2 Quản lý dữ liệu TSF (FMT_MTD)

A.3.2.1 FMT_MTD.1/AdminAct Quản lý dữ liệu TSF

FMT_MTD.1.1/AdminAct TSF phải hạn chế khả năng sửa đổi, xóa, tạo/nhập các khóa mật mã cho các quản trị viên an toàn.

Chú thích áp dụng: FMT_MTD.1.1/AdminAct chỉ nên chọn nếu các khóa mật mã có thể được sửa đổi, xóa hoặc tạo ra/nhập vào bởi quản trị viên an toàn.

A.4 Bảo vệ TSF (FPT)

A.4.1 Không an toàn (FPT_FLS)

A.4.1.1 FPT_FLS.1/LocSpace Lỗi đối với lưu giữ trạng thái an toàn

FPT_FLS.1.1/LocSpace TSF phải bảo vệ trạng thái an toàn khi xảy ra các loại lỗi sau: Không gian lưu trữ cục bộ cho dữ liệu kiểm toán đã đầy.

Chú thích áp dụng: SFR này sẽ được thêm vào nếu TOE được định cấu hình để ngăn chặn tất cả các chức năng an toàn (nghĩa là bảo vệ trạng thái an toàn) nếu không còn không gian lưu trữ cục bộ cho dữ liệu kiểm toán. Bằng cách này, kẻ tấn công sẽ không thể giấu hành động của mình bằng cách tạo ra các sự kiện kiểm toán bổ sung. Hành vi này được dự kiến sẽ được mô phỏng trong FAU_STG_EXT.1.3 trong chỉ định cuối cùng của vùng lựa chọn (nghĩa là 'tuỳ chọn khác').

A.5 Tường lửa (FFW)

A.5.1 Tường lửa lọc lưu lượng có trạng thái (FFW_RUL)

A.5.1.1 FFW_RUL_EXT.2 Lọc có trạng thái của các giao thức động

FFW_RUL_EXT.2.1 TSF phải tự động định nghĩa các quy tắc hoặc thiết lập các phiên cho phép lưu lượng mạng truyền cho các giao thức mạng sau đây [lựa chọn: *FTP, SIP, H.323; [chỉ định: các giao thức khác được hỗ trợ], không có giao thức khác*].

Chú thích áp dụng: Thành phần này đòi hỏi phải có đặc tả của các giao thức phức tạp hơn yêu cầu tường lửa cho phép lưu lượng mạng chảy nếu quy tắc hiện tại không rõ ràng cho phép dòng chảy. Ví dụ, giao thức FTP yêu cầu cả kết nối điều khiển và kết nối dữ liệu nếu người dùng chuyển các tập tin. Trong khi nhiều cổng được biết là có liên quan, cổng 21 (cổng điều khiển trên máy chủ FTP) và cổng 20 (cổng dữ liệu trên máy chủ ở chế độ hoạt động), có các cổng ngẫu nhiên> 1023 được sử dụng ở phía khách hàng. Ở chế độ thụ động, máy chủ FTP có thể sử dụng một cổng ngẫu nhiên> 1023 thay vì cổng 20. Kết nối dữ liệu được khởi tạo bởi máy khách ở chế độ thụ động và được phỏng theo bởi máy chủ FTP trong chế độ hoạt động.

Đối với các loại giao thức này, việc thiết lập kết nối "mới" là được phép, mặc dù bộ quy tắc dường như có thể phủ nhận nó (ví dụ, vì một quy tắc không thể dự đoán cổng ngẫu nhiên nào sẽ được sử dụng bởi máy khách hoặc máy chủ, quy tắc mặc định là từ chối có thể áp dụng). TSF có thể tạo ra một quy tắc động để quản lý luồng lưu lượng, hoặc TSF ngầm định cho phép kết nối mới được thiết lập dựa trên sự mong đợi của việc thực hiện giao thức như đã nêu trong RFC hoặc tiêu chuẩn tương đương.

Điều quan trọng cần lưu ý là sẽ không có bất kỳ gói tin mạng nào được kiểm tra ngoài lớp 4 (TCP/UDP). Yêu cầu này đơn giản đòi hỏi tác giả ST phải xác định các điều kiện theo đó một quy tắc được đưa vào tường lửa để cho phép các kết nối mong đợi với các cổng UDP/TCP không thể đoán trước được thiết lập chính xác.

Nếu tác giả ST bao gồm các giao thức bổ sung, họ phải xác định RFC hoặc tiêu chuẩn tương đương xác định hành vi của giao thức, như đã làm cho FTP ở trên.

Phụ lục B

(Quy định)

Các yêu cầu dựa trên lựa chọn

B.0 Giới thiệu

Như đã nêu trong phần giới thiệu về PP, các yêu cầu cơ bản (những hành động cần phải được thực hiện bởi TOE hoặc nền tảng cơ bản của TOE) bao gồm trong phần thân của tiêu chuẩn này. Có các yêu cầu bổ sung dựa trên các lựa chọn trong phần thân của PP: khi các lựa chọn nhất định được thực hiện, cần đưa vào các yêu cầu bổ sung bên dưới.

B.1 Các sự kiện kiểm toán đối với các SFR dựa trên lựa chọn

Bảng 4 - Các SFR dựa trên lựa chọn và các sự kiện có thể kiểm toán

Yêu cầu	Các sự kiện có thể kiểm toán	Nội dung ghi chép kiểm toán bổ sung
FCS_HTTPS_EXT.1	Thất bại trong việc thiết lập phiên HTTPS.	Lý do thất bại.
FCS_IPSEC_EXT.1	Thất bại trong việc thiết lập một IPsec SA.	Lý do thất bại.
FCS_SSHC_EXT.1	Thất bại trong việc thiết lập phiên SSH.	Lý do thất bại.
	Nhập lại mật khẩu SSH thành công.	Điểm cuối kết nối không phải TOE (Địa chỉ IP).
FCS_SSHS_EXT.1	Thất bại trong việc thiết lập phiên SSH.	Lý do thất bại.
	Nhập lại mật khẩu SSH thành công.	Điểm cuối kết nối không phải TOE (Địa chỉ IP).
FCS_TLSC_EXT.1	Thất bại trong việc thiết lập phiên TLS.	Lý do thất bại.
FCS_TLSC_EXT.2	Thất bại trong việc thiết lập phiên TLS.	Lý do thất bại.
FCS_TLSS_EXT.1	Thất bại trong việc thiết lập phiên TLS.	Lý do thất bại.
FCS_TLSS_EXT.2	Thất bại trong việc thiết lập phiên TLS.	Lý do thất bại.

FPT_TST_EXT.2	Tự kiểm tra thất bại.	Lý do thất bại (bao gồm định danh có chứng thư không hợp lệ).
FPT_TUD_EXT.2	Cập nhật thất bại.	Lý do thất bại (bao gồm định danh có chứng thư không hợp lệ).
FMT_MOF.1(2)/TrustedUpdate	Bật hoặc Tắt tính năng kiểm tra tự động để cập nhật hoặc tự động cập nhật.	Không.

B.2 Hỗ trợ mã hóa (FCS)

B.2.1 Giao thức mật mã (Mở rộng – FCS_HTTPS_EXT, FCS_ IPSEC_EXT, FCS_SSHC_EXT, FCS_SSHS_EXT, FCS_TLSC_EXT, FCS_TLSS_EXT)

B.2.1.1 FCS_HTTPS_EXT.1 Giao thức HTTPS

FCS_HTTPS_EXT.1.1 TSF phải thực hiện giao thức HTTPS tuân thủ các yêu cầu của RFC 2818.

Chú thích áp dụng: Tác giả ST phải cung cấp đủ chi tiết để xác định cách thức thực hiện tuân thủ các tiêu chuẩn xác định; điều này có thể được thực hiện bằng cách thêm các phần tử vào thành phần này hoặc bằng cách bổ sung thêm chi tiết trong TSS.

FCS_HTTPS_EXT.1.2 TSF phải triển khai thực hiện HTTPS thông qua TLS.

FCS_HTTPS_EXT.1.3 TSF phải [lựa chọn: *không thiết lập kết nối, yêu cầu ủy quyền để thiết lập kết nối, không có hành động khác*] nếu chứng thư không hợp lệ.

Chú thích áp dụng: Hiệu lực được xác định bởi đường dẫn chứng thư, ngày hết hạn và trạng thái thu hồi theo RFC 5280.

B.2.1.2 FCS_IPSEC_EXT.1 Giao thức IPsec

Các điểm cuối của truyền thông thiết bị mạng có thể cách xa về địa lý và logic và có thể đi qua một loạt các hệ thống có thể không đáng tin cậy khác. Chức năng an toàn của thiết bị mạng phải có khả năng bảo vệ bất kỳ lưu lượng mạng quan trọng nào (lưu lượng truy cập quản trị, lưu lượng xác thực, lưu lượng kiểm toán...). Việc triển khai thực hiện IPsec là một cách tối ưu để cung cấp một kênh truyền thông được xác thực chung giữa thiết bị mạng và một thực thể CNTT bên ngoài.

IPsec không phải là thành phần bắt buộc của tiêu chuẩn này. Nếu TOE thực hiện IPsec, cần phải có một lựa chọn tương ứng trong FTP_ITC.1 và/hoặc FTP_TRP.1 để xác định giao thức IPsec được thực hiện để bảo vệ.

IPsec là một giao thức peer to peer (mạng ngang hàng), do đó không cần phân chia thành các yêu cầu riêng biệt của máy khách và máy chủ.

FCS_IPSEC_EXT.1.1 TSF phải thực hiện kiến trúc IPsec theo quy định trong RFC 4301.

Chú thích áp dụng: RFC 4301 yêu cầu thực hiện IPsec để bảo vệ lưu lượng IP thông qua việc sử dụng Cơ sở dữ liệu Chính sách An toàn (SPD). SPD được sử dụng để xác định cách xử lý các gói tin IP: BẢO VỆ gói tin (ví dụ, mã hóa gói tin), BỎ QUA các dịch vụ IPsec (ví dụ, không mã hóa), hoặc HỦY BỎ gói tin (ví dụ, dừng gói tin). SPD có thể được thực hiện bằng nhiều cách khác nhau, bao gồm các danh sách kiểm soát truy cập router, các bộ quy tắc của tường lửa, SPD "truyền thống"... Không phụ thuộc vào chi tiết thực hiện, có một khái niệm về một "quy tắc" mà một gói tin được "đối sánh" và một hành động kết quả diễn ra.

Mặc dù phải có một phương pháp để sắp xếp các quy tắc, tuy nhiên không bắt buộc phải có một cách tiếp cận chung để sắp xếp các quy tắc, miễn là SPD có thể phân biệt các gói tin IP và áp dụng các quy tắc tương ứng. Có thể có nhiều SPD (một SPD cho mỗi giao diện mạng), nhưng điều này là không bắt buộc.

FCS_IPSEC_EXT.1.2 TSF phải có một mục nhập danh nghĩa, cuối cùng trong SPD dành cho bất cứ dữ liệu nào đã đối sánh không khớp và loại bỏ dữ liệu này.

FCS_IPSEC_EXT.1.3 TSF phải thực hiện *chế độ vận chuyển (transport mode) và [lựa chọn: chế độ đường hầm, không có chế độ khác].*

FCS_IPSEC_EXT.1.4 TSF phải thực hiện giao thức ESP trong IPsec theo quy định của RFC 4303 thông qua việc sử dụng các thuật toán mật mã AES-CBC-128, AES-CBC-256 (cả hai thuật toán được quy định trong RFC 3602) và [lựa chọn: *AES-GCM-128 (quy định trong RFC 4106) , AES-GCM-256 (quy định trong RFC 4106), không có các thuật toán khác*] cùng với một HMAC dựa trên SHA.

FCS_IPSEC_EXT.1.5 TSF phải thực hiện giao thức: [lựa chọn:

- *IKEv1, sử dụng Chế độ chính (Main mode) đối với các trao đổi trong Giai đoạn 1, theo quy định trong RFC 2407, 2408, 2409, RFC 4109, [lựa chọn: không có RFC khác quy định về số thứ tự mở rộng, RFC 4304 quy định về các số thứ tự mở rộng] và [lựa chọn: không có RFC quy định về hàm băm, RFC 4868 quy định về hàm băm];*
- *IKEv2 như được quy định trong RFC 5996 và [lựa chọn: không hỗ trợ vượt tường NAT (NAT traversal), hỗ trợ bắt buộc vượt tường NAT như đã quy định trong RFC 5996, điều 2.23)], và [lựa chọn: không có RFC quy định về hàm băm, RFC 4868 quy định về hàm băm]*

].

Chú thích áp dụng: Nếu TOE thực hiện thuật toán băm SHA-2 cho IKEv1 hoặc IKEv2, tác giả ST chọn RFC 4868. Nếu tác giả ST chọn IKEv1, FCS_IPSEC_EXT.1.15 cũng phải được bao gồm trong ST. IKEv2 được yêu cầu cho những TOE đánh giá sau quý 3 năm 2016.

FCS_IPSEC_EXT.1.6 TSF phải đảm bảo dữ liệu vận chuyển được mã hóa trong giao thức [lựa chọn: *IKEv1, IKEv2*] sử dụng các thuật toán mật mã AES-CBC-128, AES-CBC-256 theo quy định trong RFC

3602 và [lựa chọn: *AES-GCM-128, AES-GCM -256 theo quy định trong RFC 5282, không có thuật toán khác*].

Chú thích áp dụng: Chỉ có thể chọn AES-GCM-128 và AES-GCM-256 nếu IKEv2 cũng được chọn, vì không có RFC quy định AES-GCM đối với IKEv1.

FCS_IPSEC_EXT.1.7 TSF đảm bảo rằng [lựa chọn:

- *Quản trị viên an toàn có thể thiết lập thời hạn sử dụng của SA IKEv1 Giai đoạn 1 dựa trên [lựa chọn:*
    - *số byte;*
    - *khoảng thời gian, trong đó các giá trị thời gian có thể được định cấu hình trong [chỉ định: dãy số nguyên tính đến 24] giờ;*

  ];
- *Quản trị viên an toàn có thể thiết lập thời hạn sử dụng của SA IKEv2 [lựa chọn:*
    - *số byte;*
    - *khoảng thời gian, trong đó các giá trị thời gian có thể được định cấu hình trong [chỉ định: dãy số nguyên tính đến 24] giờ*

  ]

].

Chú thích áp dụng: Tác giả ST chọn các yêu cầu IKEv1 hoặc các yêu cầu IKEv2 (hoặc cả hai, tùy thuộc vào sự lựa chọn trong FCS_IPSEC_EXT.1.5). Tác giả ST chọn thời hạn sử dụng dựa trên dung lượng hoặc thời hạn sử dụng dựa trên thời gian (hoặc kết hợp cả hai). Yêu cầu này phải được thực hiện bằng cách cung cấp thời hạn sử dụng do quản trị viên an toàn thiết lập (với hướng dẫn thích hợp trong các tài liệu được AGD_OPE ủy quyền). Các giới hạn được lập trình cứng sẽ không đáp ứng được yêu cầu này. Nói chung, các chỉ dẫn để thiết lập các thông số của việc thực hiện, bao gồm thời hạn sử dụng của SA cần đưa vào tài liệu hướng dẫn thiết lập cho AGD_OPE.

FCS_IPSEC_EXT.1.8 TSF đảm bảo rằng [*lựa chọn*:

- *Quản trị viên an toàn có thể thiết lập thời hạn sử dụng của SA IKEv1 Giai đoạn 2 dựa trên [lựa chọn:*
    - *số byte;*
    - *khoảng thời gian, trong đó các giá trị thời gian có thể được định cấu hình trong [chỉ định: dãy số nguyên tính đến 8] giờ*

  ];
- *Quản trị viên an toàn có thể thiết lập thời hạn sử dụng của Child SA IKEv2 [lựa chọn:*

- *số byte;*
- *khoảng thời gian, trong đó các giá trị thời gian có thể được định cấu hình trong [chỉ định: dãy số nguyên tính đến 8] giờ*

]

].

Chú thích áp dụng: Tác giả ST chọn các yêu cầu IKEv1 hoặc các yêu cầu IKEv2 (hoặc cả hai, tùy thuộc vào sự lựa chọn trong FCS_IPSEC_EXT.1.5). Tác giả ST chọn thời hạn sử dụng dựa trên dung lượng hoặc thời hạn sử dụng dựa trên thời gian (hoặc kết hợp cả hai). Yêu cầu này phải được thực hiện bằng cách cung cấp thời hạn sử dụng do quản trị viên an toàn thiết lập (với hướng dẫn thích hợp trong các tài liệu được AGD_OPE ủy quyền). Các giới hạn được lập trình cứng sẽ không đáp ứng được yêu cầu này. Nói chung, các chỉ dẫn để thiết lập các thông số của việc thực hiện, bao gồm thời hạn sử dụng của SA cần đưa vào tài liệu hướng dẫn thiết lập cho AGD_OPE.

FCS_IPSEC_EXT.1.9 TSF phải tạo giá trị bí mật x được sử dụng trong trao đổi khóa IKE Diffie-Hellman ("x" trong g^x mod p) sử dụng bộ tạo bit ngẫu nhiên được chỉ định trong FCS_RBG_EXT.1 và có độ dài ít nhất là [chỉ định: *(một hoặc nhiều) số (các) bit ít nhất gấp đôi độ an toàn của nhóm Diffie-Hellman được thỏa thuận*].

Chú thích áp dụng: Đối với DH nhóm 19 và 20, giá trị "x" là số nhân điểm cho điểm phát G.

Vì việc thực hiện có thể cho phép các nhóm Diffie-Hellman khác nhau được thỏa thuận để sử dụng trong việc tạo lập các SA, việc xác định trong FCS_IPSEC_EXT.1.9 có thể chứa nhiều giá trị. Đối với mỗi nhóm DH được hỗ trợ, tác giả ST tham khảo Bảng 2 trong NIST SP 800-57 "Khuyến nghị về quản lý khóa - Phần 1: Tổng quát" để xác định độ mạnh an toàn ("các bit an toàn") liên quan đến nhóm DH. Mỗi giá trị duy nhất sau đó được sử dụng để điền vào chỉ định cho phần tử này. Ví dụ, giả sử việc thực hiện hỗ trợ nhóm DH 14 (2048-bit MODP) và nhóm 20 (ECDH sử dụng đường cong NIST P-384). Từ Bảng 2, giá trị các bit an toàn của nhóm 14 là 112, và nhóm 20 là 192.

FCS_IPSEC_EXT.1.10 TSF phải tạo ra các nonce để sử dụng trong các trao đổi [lựa chọn: *IKEv1, IKEv2*] độ dài [lựa chọn:

- *[chỉ định: độ mạnh an toàn liên quan đến nhóm Diffie-Hellman đã thỏa thuận];*
- *có kích thước ít nhất 128 bit và bằng ít nhất một nửa kích thước đầu ra của hàm băm giả ngẫu nhiên đã được thỏa thuận (PRF)*

].

Chú thích áp dụng: Tác giả ST phải chọn tùy chọn thứ hai đối với độ dài của nonce nếu chọn IKEv2 (vì điều này được yêu cầu trong RFC 5996). Tác giả ST có thể chọn một trong hai tùy chọn đối với IKEv1.

Vì việc thực hiện có thể cho phép các nhóm Diffie-Hellman khác nhau được thỏa thuận để sử dụng trong việc tạo lập các SA, việc xác định trong FCS_IPSEC_EXT.1.9 có thể chứa nhiều giá trị. Đối với mỗi nhóm DH được hỗ trợ, tác giả ST tham khảo Bảng 2 trong NIST SP 800-57 "Khuyến nghị về quản lý khóa - Phần 1: Tổng quát" để xác định độ mạnh an toàn ("các bit an toàn") liên quan đến nhóm DH. Mỗi giá trị duy nhất sau đó được sử dụng để điền vào chỉ định cho phần tử này. Ví dụ, giả sử việc thực hiện hỗ trợ nhóm DH 14 (2048-bit MODP) và nhóm 20 (ECDH sử dụng đường cong NIST P-384). Từ Bảng 2, giá trị các bit an toàn của nhóm 14 là 112, và nhóm 20 là 192.

Bởi vì các nonce có thể được trao đổi trước khi nhóm DH được thỏa thuận, nonce được sử dụng cần đủ lớn để hỗ trợ tất cả các đề xuất được chọn cho TOE trong trao đổi.

FCS_IPSEC_EXT.1.11 TSF phải đảm bảo rằng tất cả các giao thức IKE thực hiện các nhóm DH 14 (2048-bit MODP) và [lựa chọn: *19 (ECP ngẫu nhiên 256 bit), 5 (1536-bit MODP), 24 (2048-bit MODP với 256-bit POS), 20 (ECP ngẫu nhiên 384-bit), không có nhóm DH khác*].

Chú thích áp dụng: Lựa chọn được sử dụng để chỉ định các nhóm DH bổ sung được hỗ trợ. Điều này áp dụng cho các trao đổi IKEv1 và IKEv2. Đối với các sản phẩm đánh giá sau quý 3, 2015, yêu cầu nhóm DH 19 (ECP ngẫu nhiên 256 bit) và DH nhóm 20 (ECP ngẫu nhiên 384 bit). Lưu ý: Đối với bất kỳ nhóm DH bổ sung nào được chỉ định, nhóm này phải tuân thủ các yêu cầu (về các khóa tạm thời được thiết lập) được liệt kê trong FCS_CKM.1.

FCS_IPSEC_EXT.1.12 TSF phải đảm bảo theo mặc định rằng độ mạnh của thuật toán đối xứng (về số lượng bit trong khóa) được thương lượng để bảo vệ kết nối [lựa chọn: *IKEv1 Giai đoạn 1, IKEv2 IKE_SA*] lớn hơn hoặc tương đương độ mạnh của thuật toán đối xứng (về số lượng bit trong khóa) được thương lượng để bảo vệ kết nối [lựa chọn: *IKEv1 Giai đoạn 2, IKEv2 CHILD_SA*].

Chú thích áp dụng: Tác giả ST chọn một hoặc cả hai lựa chọn IKE dựa trên những gì được thực hiện bởi TOE. Rõ ràng, (các) phiên bản IKE được chọn phải nhất quán không chỉ trong phần tử này mà còn với các lựa chọn khác của các phần tử khác trong thành phần này. Mặc dù có thể chấp nhận khả năng này được cấu hình, cấu hình mặc định trong cấu hình được đánh giá ("ngoài phạm vi" hoặc theo hướng dẫn cấu hình trong tài liệu AGD) phải cho phép kích hoạt chức năng này.

FCS_IPSEC_EXT.1.13 TSF phải đảm bảo rằng tất cả các giao thức IKE thực hiện xác thực ngang hàng sử dụng [lựa chọn: RSA, ECDSA] sử dụng các chứng thư X.509v3 phù hợp với RFC 4945 và [lựa chọn: *Các khóa chia sẻ trước, không có phương pháp khác*].

Chú thích áp dụng: Cần có ít nhất một phương thức xác thực ngang hàng dựa trên khóa công khai để phù hợp với tiêu chuẩn này; một hoặc nhiều lược đồ khóa công khai được chọn bởi tác giả ST để phản ánh những gì được thực hiện. Tác giả ST cũng đảm bảo rằng các yêu cầu FCS thích hợp phản ánh các thuật toán được sử dụng (và các khả năng tạo khóa, nếu được cung cấp) được liệt kê để hỗ trợ các phương pháp đó. Lưu ý rằng TSS sẽ giải thích chi tiết về cách thức sử dụng các thuật toán này (ví dụ: RFC 2409 xác định ba phương pháp xác thực sử dụng khóa công khai, mỗi một hỗ trợ sẽ được

mô tả trong TSS). Xác thực ngang hàng sử dụng chứng thư ECDSA X.509v3 sẽ được yêu cầu cho các TOE đánh giá sau quý 3, 2015.

FCS_IPSEC_EXT.1.14 TSF chỉ thiết lập một kênh đáng tin cậy cho các giao thức ngang hàng có chứng thư hợp lệ.

Chú thích áp dụng: Các thuật toán chứng thực ngang hàng được hỗ trợ tương tự như FCS_IPSEC_EXT.1.1.

B.2.1.3. FCS_SSHC_EXT.1 Giao thức máy khách SSH

FCS_SSHC_EXT.1.1 TSF phải thực hiện giao thức SSH tuân thủ RFC 4251, 4252, 4253, 4254, và [lựa chọn: *5647, 5656, 6187, 6668, không có RFC khác*].

Chú thích áp dụng: Tác giả ST chọn các RFC bổ sung mà đã có yêu cầu tuân thủ. Lưu ý rằng các RFC cần phải nhất quán với các lựa chọn trong các phần tử sau của thành phần này (ví dụ, các thuật toán mật mã được phép). RFC 4253 chỉ ra các thuật toán mật mã nhất định là "ĐƯỢC YÊU CẦU". Điều này có nghĩa là việc triển khai phải bao gồm việc hỗ trợ, không phải là các thuật toán phải được kích hoạt để sử dụng. Việc đảm bảo rằng các thuật toán được chỉ định là "ĐƯỢC YÊU CẦU" nhưng không được liệt kê trong các phần tử sau của thành phần này là nằm ngoài phạm vi của hoạt động đảm bảo đối với yêu cầu này.

FCS_SSHC_EXT.1.2 TSF phải đảm bảo việc thực hiện giao thức SSH hỗ trợ các phương pháp xác thực sau đây như được mô tả trong RFC 4252: dựa trên khóa công khai và dựa trên mật khẩu.

FCS_SSHC_EXT.1.3 TSF phải đảm bảo rằng, như được mô tả trong RFC 4253, các gói tin lớn hơn [chỉ định: *số byte*] byte trong kết nối vận chuyển SSH bị loại bỏ.

Chú thích áp dụng: RFC 4253 quy định việc chấp nhận "các gói tin lớn" với thông báo trước rằng các gói tin nên có "độ dài hợp lý" hoặc bị loại bỏ. Việc chỉ định phải được điền bởi tác giả ST với kích thước gói tin tối đa được chấp nhận, do đó xác định "độ dài hợp lý" cho TOE.

FCS_SSHC_EXT.1.4 TSF phải đảm bảo rằng việc thực hiện vận chuyển SSH sử dụng các thuật toán mã hóa sau và từ chối tất cả các thuật toán mã hóa khác: *aes128-cbc, aes256-cbc, [lựa chọn: AEAD_AES_128_GCM, AEAD_AES_256_GCM, không có thuật toán khác]*.

Chú thích áp dụng: RFC 5647 chỉ định việc sử dụng thuật toán AEAD_AES_128_GCM và AEAD_AES_256_GCM trong SSH. Như được quy định trong RFC 5647, AEAD_AES_128_GCM và AEAD_AES_256_GCM chỉ có thể được chọn làm thuật toán mã hóa khi cùng một thuật toán được sử dụng như là thuật toán MAC. Trong chỉ định, tác giả ST có thể chọn các thuật toán AES-GCM, hoặc "không có các thuật toán khác" nếu AES-GCM không được hỗ trợ. Nếu AES-GCM được chọn, nên có các mục FCS_COP tương ứng trong ST.

FCS_SSHC_EXT.1.5 TSF phải đảm bảo rằng việc triển khai vận chuyển SSH sử dụng *[lựa chọn: ssh-rsa, ecdsa-sha2-nistp256]* và *[lựa chọn: ecdsa-sha2-nistp384, x509v3- ecdsa-sha2-nistp256, x509v3-*

ecdsa-sha2-nistp384, không có các thuật toán khóa công khai khác] làm thuật toán khóa công khai của nó và loại bỏ tất cả các thuật toán khóa công khai khác.

Chú thích áp dụng: Các triển khai chỉ chọn ssh-rsa sẽ không đạt được độ an toàn 112-bit trong quá trình tạo chữ ký số để xác thực SSH như được đề nghị trong NIST SP 800-131A. Các phiên bản trong tương lai của PP này có thể loại bỏ ssh-rsa làm lựa chọn. Nếu chọn x509v3-ecdsa- sha2-nistp256 hoặc x509v3-ecdsa-sha2-nistp384 thì danh sách các cơ quan chứng thực tin cậy phải được chọn trong FCS_SSHC_EXT.1.9.

FCS_SSHC_EXT.1.6 TSF phải đảm bảo rằng việc triển khai vận chuyển SSH sử dụng *[lựa chọn: hmac-sha1, hmac-sha1-59] và [lựa chọn: AEAD_AES_128_GCM, không có thuật toán MAC khác]* như là thuật toán MAC đảm bảo toàn vẹn dữ liệu của nó và từ chối tất cả các thuật toán MAC khác.

Chú thích áp dụng: RFC 5647 chỉ định việc sử dụng thuật toán AEAD_AES_128_GCM và AEAD_AES_256_GCM trong SSH. Như được quy định trong RFC 5647, AEAD_AES_128_GCM và AEAD_AES_256_GCM chỉ có thể được chọn làm thuật toán MAC khi thuật toán tương tự đang được sử dụng làm thuật toán mã hóa. RFC 6668 chỉ định việc sử dụng các thuật toán sha2 trong SSH.

FCS_SSHC_EXT.1.7 TSF phải đảm bảo rằng *[lựa chọn: Diffie-Hellman-group14-sha1, ecdh-sha2-nistp256] và [lựa chọn: ecdh-sha2-nistp384, ecdh-sha2-nistp521, không có phương pháp khác]* là phương pháp trao đổi khóa được sử dụng cho giao thức SSH.

FCS_SSHC_EXT.1.8 TSF phải đảm bảo rằng kết nối SSH được khóa lại sau khi không có hơn 2^28 gói tin đã được truyền bằng khóa đó.

FCS_SSHC_EXT.1.9 TSF phải đảm bảo rằng máy khách SSH xác thực định danh của máy chủ SSH bằng cách sử dụng cơ sở dữ liệu cục bộ liên kết mỗi tên máy chủ với khóa công khai tương ứng hoặc *[lựa chọn: một danh sách các cơ quan chứng thực tin cậy, không có phương pháp khác]* như được mô tả trong RFC 4251 điều 4.1.

Chú thích áp dụng: Danh sách các cơ quan chứng thực tin cậy chỉ có thể được chọn nếu x509v3-ecdsa-sha2-nistp256 hoặc x509v3-ecdsa-sha2-nistp384 được chọn trong FCS_SSHC_EXT.1.5.

B.2.1.4 Giao thức máy chủ FCS_SSHS_EXT.1 SSH

FCS_SSHS_EXT.1.1 TSF thực hiện giao thức SSH tuân thủ các RFC 4251, 4252, 4253, 4254, và [lựa chọn: *5647, 5656, 6187, 6668, không có RFC khác*].

Chú thích áp dụng: Tác giả ST chọn các RFC bổ sung mà đã có yêu cầu tuân thủ. Lưu ý rằng những điều này cần phải nhất quán với các lựa chọn trong các phần tử sau của thành phần này (ví dụ, các thuật toán mật mã được phép). RFC 4253 chỉ ra rằng một số thuật toán mật mã nhất định "ĐƯỢC YÊU CẦU". Điều này có nghĩa là việc triển khai phải bao gồm hỗ trợ chứ không phải là các thuật toán phải được kích hoạt để sử dụng. Việc đảm bảo rằng các thuật toán được chỉ định là "ĐƯỢC YÊU

CẦU" nhưng không được liệt kê trong các phần tử sau của thành phần này nằm ngoài phạm vi của hoạt động đảm bảo cho yêu cầu này.

FCS_SSHS_EXT.1.2 TSF phải đảm bảo rằng việc thực hiện giao thức SSH hỗ trợ các phương pháp xác thực sau đây như được mô tả trong RFC 4252: dựa trên khóa công khai, dựa trên mật khẩu.

FCS_SSHS_EXT.1.3 TSF phải đảm bảo rằng, như được mô tả trong RFC 4253, các gói tin lớn hơn [chỉ định: *số byte*] byte trong kết nối vận chuyển SSH bị loại bỏ.

Chú thích áp dụng: RFC 4253 quy định việc chấp nhận "các gói tin lớn" với thông báo trước rằng các gói tin nên có "độ dài hợp lý" hoặc bị loại bỏ. Việc chỉ định phải được điền bởi tác giả ST với kích thước gói tin tối đa được chấp nhận, do đó xác định "độ dài hợp lý" cho TOE.

FCS_SSHS_EXT.1.4 TSF phải đảm bảo rằng việc thực hiện vận chuyển SSH sử dụng các thuật toán mã hóa sau đây và từ chối tất cả các thuật toán mã hóa khác: *aes128-cbc, aes256-cb, [lựa chọn: AEAD_AES_128_GCM, AEAD_AES_256_GCM, không có thuật toán khác]*.

Chú thích áp dụng: RFC 5647 chỉ định việc sử dụng thuật toán AEAD_AES_128_GCM và AEAD_AES_256_GCM trong SSH. Như được mô tả trong RFC 5647, AEAD_AES_128_GCM và AEAD_AES_256_GCM chỉ có thể được chọn làm thuật toán mã hóa khi thuật toán tương tự đang được sử dụng làm thuật toán MAC. Trong chỉ định, tác giả ST có thể chọn các thuật toán AES-GCM, hoặc "không có các thuật toán khác" nếu AES-GCM không được hỗ trợ. Nếu AES-GCM được chọn, nên có các mục nhập FCS_COP tương ứng trong ST.

FCS_SSHS_EXT.1.5 TSF phải đảm bảo rằng việc triển khai vận chuyển SSH sử dụng *[lựa chọn: ssh-rsa, ecdsa-sha2-nistp256] và [lựa chọn: ecdsa-sha2-nistp384, x509v3- ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, không có các thuật toán khóa công khai khác]* làm thuật toán khóa công khai của nó và loại bỏ tất cả các thuật toán khóa công khai khác.

Chú thích áp dụng: Các triển khai chỉ chọn ssh-rsa sẽ không đạt được độ an toàn 112-bit trong quá trình tạo chữ ký số để xác thực SSH như được đề nghị trong NIST SP 800-131A. Các phiên bản trong tương lai của PP này có thể loại bỏ ssh-rsa làm lựa chọn.

FCS_SSHS_EXT.1.6 TSF phải đảm bảo rằng việc thực hiện vận chuyển SSH sử dụng *[lựa chọn: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512] và [lựa chọn: AEAD_AES_128_GCM, AEAD_AES_256_GCM, không có thuật toán MAC khác]* như là thuật toán MAC của nó và từ chối tất cả các thuật toán MAC khác.

Chú thích áp dụng: RFC 5647 chỉ định việc sử dụng thuật toán AEAD_AES_128_GCM và AEAD_AES_256_GCM trong SSH. Như được quy định trong RFC 5647, AEAD_AES_128_GCM và AEAD_AES_256_GCM chỉ có thể được chọn làm thuật toán MAC khi thuật toán tương tự đang được sử dụng làm thuật toán mã hóa. RFC 6668 chỉ định việc sử dụng các thuật toán sha2 trong SSH.

FCS_SSHS_EXT.1.7 TSF phải đảm bảo rằng *[lựa chọn: Diffie-Hellman-group14-sha1, ecdh-sha2-nistp256] và [lựa chọn: ecdh-sha2-nistp384, ecdh-sha2-nistp521, không có phương pháp khác]* là phương pháp trao đổi khóa được sử dụng cho giao thức SSH.

FCS_SSHS_EXT.1.8 TSF phải đảm bảo rằng kết nối SSH được khóa lại sau khi không có hơn 2^28 gói tin đã được truyền bằng khóa đó.

B.2.1.5 FCS_TLSC_EXT.1 Giao thức máy khách TLS

TLS không phải là thành phần bắt buộc của tiêu chuẩn này. Nếu TOE thực hiện IPsec, cần phải có một lựa chọn tương ứng trong FTP_ITC.1 và / hoặc FTP_TRP.1 để xác định giao thức TLS được thực hiện để bảo vệ.

TOE có thể hoạt động như là máy khách, máy chủ, hoặc cả hai trong các phiên TLS. Yêu cầu đã được tách thành các yêu cầu đối với máy khách TLS (FCS_TLSC_EXT) và máy chủ TLS (FCS_TLSS_EXT) để phù hợp với những khác biệt này. Nếu TOE đóng vai trò máy khách trong các phiên TLS đã được xác nhận, tác giả ST nên xác định tuân thủ một trong các yêu cầu FCS_TLSC_EXT.

Ngoài ra, TLS có thể có hoặc không được thực hiện với việc xác thực máy khách. Tác giả ST sẽ yêu cầu FCS_TLSC_EXT.1 và FCS_TLSS_EXT.1 nếu TOE không hỗ trợ xác thực máy khách. Tác giả ST nên yêu cầu FCS_TLSC_EXT.2 và FCS_TLSS_EXT.2 nếu việc xác thực máy khách được thực hiện bởi TOE. Nếu TLS được chọn là một phương tiện để cung cấp một kênh giao tiếp đáng tin cậy cho một thực thể IT bên ngoài trong FTP_ITC.1, thì FCS_TLSC_EXT.2 là bắt buộc.

FCS_TLSC_EXT.1.1 TSF phải thực hiện [lựa chọn: *TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] hỗ trợ các ciphersuites sau đây:

- *Ciphersuites bắt buộc:*
    - *TLS_RSA_WITH_AES_128_CBC_SHA như quy định trong RFC 3268*
- *[lựa chọn: Ciphersuites tùy chọn:*
    - *TLS_RSA_WITH_AES_256_CBC_SHA như quy định trong RFC 3268*
    - *TLS_RSA_WITH_AES_256_CBC_SHA như quy định trong RFC 3268*
    - *TLS_DHE_RSA_WITH_AES_128_CBC_SHA như quy định trong RFC 3268*
    - *TLS_DHE_RSA_WITH_AES_256_CBC_SHA như quy định trong RFC 3268*
    - *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA như quy định trong RFC 4492*
    - *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA như quy định trong RFC 4492*
    - *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA như quy định trong RFC 4492*
    - *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA như quy định trong RFC 4492*
    - *TLS_RSA_WITH_AES_128_CBC_SHA256 như quy định trong RFC 5246*

- *TLS_RSA_WITH_AES_256_CBC_ SHA256 như quy định trong RFC 5246*
- *TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 như quy định trong RFC 5246*
- *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 như quy định trong RFC 5246*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 như quy định trong RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 như quy định trong RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 như quy định trong RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 như quy định trong RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 như quy định trong RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 như quy định trong RFC 5289*
- *Không có ciphersuite khác].*

Chú thích áp dụng: Các ciphersuites được kiểm tra trong cấu hình đánh giá sẽ bị giới hạn theo yêu cầu này. Tác giả ST cần chọn các ciphersuites tùy chọn được hỗ trợ; nếu không có ciphersuites nào được hỗ trợ ngoài các dãy bắt buộc, thì sẽ lựa chọn "Không". Cần hạn chế các ciphersuites có thể được sử dụng trong một cấu hình đánh giá quản trị trên máy chủ trong môi trường thử nghiệm.

TLS_RSA_WITH_AES_128_CBC_SHA là bắt buộc để đảm bảo tuân thủ RFC 5246.

Các yêu cầu này sẽ được xem xét lại khi các phiên bản TLS mới được tiêu chuẩn hóa bởi IETF.

Trong một phiên bản tương lai của PP, sẽ yêu cầu bắt buộc TLS v1.2 cho tất cả TOE.

FCS_TLSC_EXT.1.2 TSF phải xác minh định danh đưa ra có khớp với định danh tham chiếu theo RFC 6125.

Chú thích áp dụng: Các quy tắc xác minh định danh được mô tả trong Điều 6 của RFC 6125. Định danh tham chiếu do người dùng thiết lập (ví dụ như nhập một URL vào trình duyệt web hoặc nhấp vào một liên kết) thông qua cấu hình (ví dụ như cấu hình tên của máy chủ thư hoặc máy chủ xác thực), hoặc bằng một ứng dụng (ví dụ như một tham số của một API) tùy thuộc vào dịch vụ ứng dụng. Dựa vào tên miền nguồn của định danh tham chiếu đơn và loại dịch vụ ứng dụng (ví dụ HTTP, SIP, LDAP), máy khách sẽ thiết lập tất cả các định danh tham chiếu được chấp nhận, chẳng hạn như Tên chung cho trường Tên chủ thể của chứng thư và một Tên DNS, tên URI và tên Dịch vụ (phân biệt sự khác nhau giữa chữ hoa và chữ thường) cho trường Subject Alternative Name. Sau đó máy khách sẽ so sánh danh sách tất cả các định danh tham chiếu có thể chấp nhận được với định danh được trình bày trong chứng thư của máy chủ TLS.

Phương pháp ưu tiên được sử dụng để xác minh là Subject Alternative Name sử dụng tên DNS, tên URI hoặc tên Dịch vụ. Việc xác minh sử dụng Tên chung là yêu cầu bắt buộc vì các mục đích tương thích ngược. Ngoài ra, việc hỗ trợ sử dụng các địa chỉ IP trong Tên chủ thể hoặc Subject Alternative Name sẽ không được khuyến khích vì trái lại các hướng dẫn thực hành tốt nhất, nhưng cũng có thể

được thực hiện. Cuối cùng, máy khách phải tránh hình thành các định danh tham chiếu sử dụng các ký tự đại diện. Tuy nhiên, nếu các định danh được trình bày bao gồm các ký tự đại diện, máy khách sẽ phải tuân thủ các hướng dẫn thực hành tốt nhất về sự tương hợp, so khớp; những hướng dẫn thực hành tốt nhất này được ghi nhận trong hoạt động đảm bảo.

FCS_TLSC_EXT.1.3 TSF chỉ thiết lập một kênh đáng tin cậy nếu có chứng thư ngang hàng hợp lệ.

Chú thích áp dụng: Tính hiệu lực được xác định bằng xác minh định danh, đường dẫn chứng thư, ngày hết hạn và trạng thái thu hồi theo RFC 5280. Thời hạn hiệu lực của chứng thư được kiểm tra tuân theo thử nghiệm được thực hiện cho FIA_X509_EXT.1.

FCS_TLSC_EXT.1.4 TSF phải trình bày Supported Elliptic Curves Extension - Mở rộng đường cong Elliptic được hỗ trợ trong Client Hello với các đường cong NIST sau đây: *[lựa chọn: secp256r1, secp384r1, secp521r1, hoặc không]* và không có các đường cong khác.

Chú thích áp dụng: Nếu các ciphersuites cùng các đường cong Elliptic được chọn trong FCS_TLSC_EXT.1.1, thì cần phải chọn một hoặc nhiều đường cong. Nếu không lựa chọn các ciphersuites cùng các đường cong elliptic trong FCS_TLS_EXT.1.1, thì sẽ lựa chọn 'không'.

Yêu cầu này giới hạn các đường cong Elliptic được cho phép để xác thực và thỏa thuận khóa với các đường cong NIST từ FCS_COP.1(2) và FCS_CKM.1 và FCS_CKM.2. Phần mở rộng này là bắt buộc đối với máy khách hỗ trợ các ciphersuites đường cong Elliptic.

B.2.1.6 FCS_TLSC_EXT.2 Giao thức máy khách TLS có xác thực

(Xem đoạn giới thiệu trong điều B.2.1.5)

FCS_TLSC_EXT.2.1 TSF phải thực hiện [lựa chọn: *TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] hỗ trợ các ciphersuites sau đây:

- *Ciphersuites bắt buộc:*
    - *TLS_RSA_WITH_AES_128_CBC_SHA như quy định trong RFC 3268*
- *[lựa chọn: Ciphersuites tùy chọn:*
    - *TLS_RSA_WITH_AES_256_CBC_SHA như quy định trong RFC 3268*
    - *TLS_DHE_RSA_WITH_AES_128_CBC_SHA như quy định trong RFC 3268*
    - *TLS_DHE_RSA_WITH_AES_256_CBC_SHA như quy định trong RFC 3268*
    - *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA như quy định trong RFC 4492*
    - *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA như quy định trong RFC 4492*
    - *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA như quy định trong RFC 4492*
    - *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA như quy định trong RFC 4492*
    - *TLS_RSA_WITH_AES_128_CBC_SHA256 như quy định trong RFC 5246*

- *TLS_RSA_WITH_AES_256_CBC_ SHA256 như quy định trong RFC 5246*
- *TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 như quy định trong RFC 5246*
- *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 như quy định trong RFC 5246*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 như quy định trong RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 như quy định trong RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 như quy định trong RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 như quy định trong RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 như quy định trong RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 như quy định trong RFC 5289*
- *Không có ciphersuite khác].*

Chú thích áp dụng: Các ciphersuites được kiểm tra trong cấu hình đánh giá sẽ bị giới hạn theo yêu cầu này. Tác giả ST cần chọn các ciphersuites tùy chọn được hỗ trợ; nếu không có ciphersuites nào được hỗ trợ ngoài các dãy bắt buộc, thì sẽ lựa chọn "Không". Cần hạn chế các ciphersuites có thể được sử dụng trong một cấu hình đánh giá quản trị trên máy chủ trong môi trường thử nghiệm. Các thuật toán Dãy B liệt kê ở trên (RFC 6460) là các thuật toán được ưu tiên để thực hiện. TLS_RSA_WITH_AES_128_CBC_SHA là bắt buộc để đảm bảo tuân thủ RFC 5246.

Các yêu cầu này sẽ được xem xét lại khi các phiên bản TLS mới được tiêu chuẩn hóa bởi IETF.

Trong một phiên bản tương lai của PP, sẽ yêu cầu bắt buộc TLS v1.2 cho tất cả TOE.

FCS_TLSC_EXT.2.2 TSF phải xác minh định danh đưa ra phù hợp với định danh tham chiếu theo RFC 6125.

Chú thích áp dụng: Các quy tắc xác minh định danh được mô tả trong Điều 6 của RFC 6125. Định danh tham chiếu do người dùng thiết lập (ví dụ như nhập URL vào trình duyệt web hoặc nhấp vào một liên kết) thông qua cấu hình (ví dụ như cấu hình tên của máy chủ thư hoặc máy chủ xác thực), hoặc bằng một ứng dụng (ví dụ như một tham số của một API) tùy thuộc vào dịch vụ ứng dụng. Dựa vào tên miền nguồn của định danh tham chiếu đơn và loại dịch vụ ứng dụng (ví dụ HTTP, SIP, LDAP), máy khách sẽ thiết lập tất cả các định danh tham chiếu được chấp nhận, chẳng hạn như Tên chung cho trường Tên chủ thể của chứng thư và một Tên DNS, tên URI và tên Dịch vụ (phân biệt sự khác nhau giữa chữ hoa và chữ thường) cho trường Subject Alternative Name. Sau đó máy khách sẽ so sánh danh sách tất cả các định danh tham chiếu có thể chấp nhận được với các định danh được trình bày trong chứng thư của máy chủ TLS.

Phương pháp ưu tiên được sử dụng để xác minh là Subject Alternative Name sử dụng tên DNS, tên URI hoặc tên Dịch vụ. Việc xác minh sử dụng Tên chung là yêu cầu bắt buộc vì các mục đích tương thích ngược. Ngoài ra, việc hỗ trợ sử dụng các địa chỉ IP trong Tên chủ thể hoặc Subject Alternative

Name sẽ không được khuyến khích vì trái lại các hướng dẫn thực hành tốt nhất, nhưng cũng có thể được thực hiện. Cuối cùng, máy khách phải tránh hình thành các định danh tham chiếu sử dụng các ký tự đại diện. Tuy nhiên, nếu các định danh được trình bày bao gồm các ký tự đại diện, máy khách sẽ phải tuân thủ các hướng dẫn thực hành tốt nhất về sự tương hợp, so khớp; những hướng dẫn thực hành tốt nhất này được ghi nhận trong hoạt động đảm bảo.

FCS_TLSC_EXT.2.3 TSF chỉ thiết lập một kênh đáng tin cậy nếu có chứng thư ngang hàng hợp lệ.

Chú thích áp dụng: Tính hiệu lực được xác định bằng xác minh định danh, đường dẫn chứng thư, ngày hết hạn và trạng thái thu hồi theo RFC 5280. Thời hạn hiệu lực của chứng thư được kiểm tra tuân theo thử nghiệm được thực hiện cho FIA_X509_EXT.1.

FCS_TLSC_EXT.2.4 TSF phải trình bày Supported Elliptic Curves Extension - Mở rộng đường cong Elliptic được hỗ trợ trong Client Hello với các đường cong NIST sau đây: *[lựa chọn: secp256r1, secp384r1, secp521r1, hoặc không]* và không có các đường cong khác.

Chú thích áp dụng: Nếu các ciphersuites cùng các đường cong Elliptic được chọn trong FCS_TLSC_EXT.2.1, thì cần phải chọn một hoặc nhiều đường cong. Nếu không lựa chọn các ciphersuites cùng các đường cong elliptic trong FCS_TLS_EXT.2.1, thì sẽ lựa chọn 'không'.

Yêu cầu này giới hạn các đường cong Elliptic được cho phép để xác thực và thỏa thuận khóa với các đường cong NIST từ FCS_COP.1(2) và FCS_CKM.1 và FCS_CKM.2. Phần mở rộng này là bắt buộc đối với máy khách hỗ trợ các ciphersuites đường cong Elliptic.

FCS_TLSC_EXT.2.5 TSF phải hỗ trợ xác thực lẫn nhau sử dụng các chứng thư X.509v3.

Chú thích áp dụng: Việc sử dụng các chứng thư X.509v3 cho TLS được đề cập trong FIA_X509_EXT.2.1. Yêu cầu này cho biết thêm rằng máy khách phải có khả năng trình bày chứng thư cho một máy chủ TLS vì mục đích xác thực lẫn nhau TLS.

B.1.2.7 FCS_TLSS_EXT.1 Giao thức máy chủ TLS

Như đã nêu trong điều B.2.1.5, TOE có thể hoạt động như một máy khách, máy chủ, hoặc giữ vai trò của cả hai trong các phiên TLS. Nếu TOE hoạt động như máy chủ trong các phiên TLS đã được xác nhận (FTP_ITC.1 hoặc FTP_TRP.1), thì tác giả ST phải xác nhận một trong các yêu cầu FCS_TLSS_EXT.

TLS có thể có hoặc không thực hiện thông qua phương thức xác thực lẫn nhau. Tác giả ST sẽ yêu cầu FCS_TLSS_EXT.1 nếu TOE không hỗ trợ xác thực lẫn nhau. Tác giả ST sẽ yêu cầu FCS_TLSS_EXT.2 nếu TOE có hỗ trợ xác thực lẫn nhau.

FCS_TLSS_EXT.1.1 TSF phải thực hiện [lựa chọn: *TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] hỗ trợ các ciphersuites sau đây:

- *Ciphersuites bắt buộc:*

- *TLS_RSA_WITH_AES_128_CBC_SHA như quy định trong RFC 3268*

- *[lựa chọn: Ciphersuites tùy chọn:*
  - *TLS_RSA_WITH_AES_256_CBC_SHA như quy định trong RFC 3268*
  - *TLS_DHE_RSA_WITH_AES_128_CBC_SHA như quy định trong RFC 3268*
  - *TLS_DHE_RSA_WITH_AES_256_CBC_SHA như quy định trong RFC 3268*
  - *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA như quy định trong RFC 4492*
  - *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA như quy định trong RFC 4492*
  - *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA như quy định trong RFC 4492*
  - *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA như quy định trong RFC 4492*
  - *TLS_RSA_WITH_AES_128_CBC_SHA256 như quy định trong RFC 5246*
  - *TLS_RSA_WITH_AES_256_CBC_ SHA256 như quy định trong RFC 5246*
  - *TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 như quy định trong RFC 5246*
  - *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 như quy định trong RFC 5246*
  - *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 như quy định trong RFC 5289*
  - *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 như quy định trong RFC 5289*
  - *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 như quy định trong RFC 5289*
  - *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 như quy định trong RFC 5289*
  - *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 như quy định trong RFC 5289*
  - *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 như quy định trong RFC 5289*
  - *Không có ciphersuite khác].*

Chú thích áp dụng: Các ciphersuites được kiểm tra trong cấu hình đánh giá sẽ bị giới hạn theo yêu cầu này. Tác giả ST cần chọn các ciphersuites tùy chọn được hỗ trợ; nếu không có ciphersuites nào được hỗ trợ ngoài các dãy bắt buộc, thì sẽ lựa chọn "Không". Cần hạn chế các ciphersuites có thể được sử dụng trong một cấu hình đánh giá quản trị trên máy chủ trong môi trường thử nghiệm. TLS_RSA_WITH_AES_128_CBC_SHA là bắt buộc để đảm bảo tuân thủ RFC 5246.

Các yêu cầu này sẽ được xem xét lại khi các phiên bản TLS mới được tiêu chuẩn hóa bởi IETF.

Trong một phiên bản tương lai của PP, sẽ yêu cầu bắt buộc TLS v1.2 cho tất cả TOE.

FCS_TLSS_EXT.2.2 TSF phải từ chối các kết nối từ các máy khách yêu cầu SSL 1.0, SSL 2.0, SSL 3.0, TLS 1.0, và [lựa chọn: *TLS 1.1, TLS 1.2, không*].

Chú thích áp dụng: Tất cả các phiên bản SSL và TLS v1.0 đều bị từ chối. Bất kỳ phiên bản TLS nào không được lựa chọn trong FCS_TLSS_EXT.1.1 đều phải được chọn ở đây.

FCS_TLSS_EXT.1.3 TSF phải tạo ra các tham số thiết lập khóa bằng cách sử dụng RSA với kích thước khóa 2048 bit và [lựa chọn: *3072 bit, 4096 bit, không có kích thước khác*] và *[lựa chọn: trên các đường cong NIST [lựa chọn: secp256r1, secp384r1] và không có các đường cong khác; các thông số Diffie-Hellman với kích thước 2048 bit và [lựa chọn: 3072 bit, không có kích thước khác]; không chọn bit khác].*

Chú thích áp dụng: Nếu ST liệt kê một ciphersuite DHE hoặc ECDHE trong FCS_TLSS_EXT.1.1, ST phải bao gồm lựa chọn Diffie-Hellman hoặc lựa chọn các đường cong NIST theo yêu cầu. FMT_SMF.1 đòi hỏi cấu hình các tham số thỏa thuận khóa để thiết lập độ mạnh an toàn của kết nối TLS.

B.2.1.8 FCS_TLSS_EXT.2 Giao thức máy chủ TLS có xác thực lẫn nhau

(Xem đoạn giới thiệu trong điều B.2.1.7)

FCS_TLSS_EXT.2.1 TSF phải thực hiện [lựa chọn: *TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] hỗ trợ các ciphersuites sau đây:

- *Ciphersuites bắt buộc:*
    - *TLS_RSA_WITH_AES_128_CBC_SHA như quy định trong RFC 3268*
- *[lựa chọn: Ciphersuites tùy chọn:*
    - *TLS_RSA_WITH_AES_256_CBC_SHA như quy định trong RFC 3268*
    - *TLS_DHE_RSA_WITH_AES_128_CBC_SHA như quy định trong RFC 3268*
    - *TLS_DHE_RSA_WITH_AES_256_CBC_SHA như quy định trong RFC 3268*
    - *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA như quy định trong RFC 4492*
    - *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA như quy định trong RFC 4492*
    - *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA như quy định trong RFC 4492*
    - *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA như quy định trong RFC 4492*
    - *TLS_RSA_WITH_AES_128_CBC_SHA256 như quy định trong RFC 5246*
    - *TLS_RSA_WITH_AES_256_CBC_ SHA256 như quy định trong RFC 5246*
    - *TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 như quy định trong RFC 5246*
    - *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 như quy định trong RFC 5246*
    - *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 như quy định trong RFC 5289*
    - *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 như quy định trong RFC 5289*
    - *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 như quy định trong RFC 5289*

- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 như quy định trong RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 như quy định trong RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 như quy định trong RFC 5289*
- *Không có ciphersuite khác].*

Chú thích áp dụng: Các ciphersuites được kiểm tra trong cấu hình đánh giá sẽ bị giới hạn theo yêu cầu này. Tác giả ST cần chọn các ciphersuites tùy chọn được hỗ trợ; nếu không có ciphersuites nào được hỗ trợ ngoài các dãy bắt buộc, thì sẽ lựa chọn "Không". Cần hạn chế các ciphersuites có thể được sử dụng trong một cấu hình đánh giá quản trị trên máy chủ trong môi trường thử nghiệm. Các thuật toán Dãy B liệt kê ở trên (RFC 6460) là các thuật toán được ưu tiên để thực hiện. TLS_RSA_WITH_AES_128_CBC_SHA là bắt buộc để đảm bảo tuân thủ RFC 5246.

Các yêu cầu này sẽ được xem xét lại khi các phiên bản TLS mới được tiêu chuẩn hóa bởi IETF.

Trong một phiên bản tương lai của PP, sẽ yêu cầu bắt buộc TLS v1.2 cho tất cả TOE.

FCS_TLSS_EXT.2.2 TSF phải từ chối các kết nối từ các máy khách yêu cầu SSL 1.0, SSL 2.0, SSL 3.0, TLS 1.0, và [lựa chọn: *TLS 1.1, TLS 1.2, không*].

Chú thích áp dụng: Tất cả các phiên bản SSL và TLS v1.0 đều bị từ chối. Bất kỳ phiên bản TLS nào không được lựa chọn trong FCS_TLSS_EXT.1.1 đều phải được chọn ở đây.

FCS_TLSS_EXT.2.3 TSF phải tạo ra các tham số thiết lập khóa bằng cách sử dụng RSA với kích thước khóa 2048 bit và [lựa chọn: *3072 bit, 4096 bit, không có kích thước khác*] và *[lựa chọn: trên các đường cong NIST [lựa chọn: secp256r1, secp384r1] và không có các đường cong khác; các thông số Diffie-Hellman với kích thước 2048 bit và [lựa chọn: 3072 bit, không có kích thước khác]; không chọn bit khác].*

Chú thích áp dụng: Nếu ST liệt kê một ciphersuite DHE hoặc ECDHE trong FCS_TLSS_EXT.2.1, ST phải bao gồm lựa chọn Diffie-Hellman hoặc lựa chọn các đường cong NIST theo yêu cầu. FMT_SMF.1 đòi hỏi cấu hình các tham số thỏa thuận khóa để thiết lập độ mạnh an toàn của kết nối TLS.

FCS_TLSS_EXT.2.4 TSF phải hỗ trợ các máy khách TLS xác thực lẫn nhau sử dụng các chứng thư X.509v3.

FCS_TLSS_EXT.2.5 TSF chỉ thiết lập một kênh đáng tin cậy nếu có chứng thư ngang hàng hợp lệ.

Chú thích áp dụng: Việc sử dụng các chứng thư X.509v3 cho TLS được đề cập trong FIA_X509_EXT.2.1. Yêu cầu này cho biết thêm rằng việc sử dụng phải bao gồm cả hỗ trợ các chứng thư số vì mục đích xác thực lẫn nhau TLS.

Tính hiệu lực được xác định bằng đường dẫn chứng thư, ngày hết hạn và trạng thái thu hồi theo RFC 5280. Thời hạn hiệu lực của chứng thư được kiểm tra tuân theo thử nghiệm được thực hiện cho FIA_X509_EXT.1.

FCS_TLSS_EXT.2.6 TSF phải không thiết lập một kênh đáng tin cậy nếu tên phân biệt (DN) hoặc Subject Alternative Name (SAN) có trong một chứng thư không khớp với định danh dự kiến của chứng thư ngang hàng.

Chú thích áp dụng: Định danh ngang hàng có thể nằm trong trường Chủ thể hoặc phần mở rộng Subject Alternative Name của chứng thư. Định danh mong muốn có thể hoặc được cấu hình, hoặc được so sánh với Tên miền, địa chỉ IP, tên người dùng hoặc địa chỉ email được sử dụng bởi thiết bị ngang hàng, hoặc cũng có thể được chuyển đến một máy chủ thư mục để so sánh. Trùng khớp phải được thực hiện bằng cách so sánh từng bit.

B.3 Bảo vệ TSF (FPT)

B.3.1 Tự kiểm thử TSF (Mở rộng)

B.3.1.1 FPT_TST_EXT.2 Tự kiểm thử dựa trên các chứng thư

FPT_TST_EXT.2.1 TSF phải thất bại trong tự kiểm thử nếu một chứng thư được dùng để tự kiểm thử và chứng thư tương ứng được coi là không hợp lệ.

Chú thích áp dụng: Các chứng thư có thể được sử dụng tùy ý để tự kiểm thử (FPT_TST_EXT.1.1). Phần tử này phải được bao gồm trong ST nếu sử dụng các chứng thư để tự kiểm thử. Nếu "code signing cho xác thực tính toàn vẹn" được lựa chọn trong FIA_X509_EXT.2.1, thì phải bao gồm FPT_TST_EXT.2 trong ST.

Tính hiệu lực được xác định bằng đường dẫn chứng thư, ngày hết hạn và trạng thái thu hồi theo FIA_X509_EXT.1.

B.3.2 Cập nhật tin cậy (FPT_TUD_EXT)

B.3.2.1 FPT_TUD_EXT.2 Cập nhật tin cậy dựa trên các chứng thư

FPT_TUD_EXT.2.1 TSF phải không cài đặt bản cập nhật nếu chứng thư số được coi là không hợp lệ.

FPT_TUD_EXT.2.2 Khi chứng thư được coi là không hợp lệ vì đã hết hạn, TSF phải [lựa chọn: *cho phép quản trị viên lựa chọn chấp nhận chứng thư trong những trường hợp này, chấp nhận chứng thư, không chấp nhận chứng thư*].

Chú thích áp dụng: Các chứng thư có thể được sử dụng tùy ý cho code signing của các bản cập nhật phần mềm hệ thống (FPT_TUD_EXT.1.3). Phần tử này phải được bao gồm trong ST nếu sử dụng các chứng thư để xác nhận bản cập nhật. Nếu "code signing cho các bản cập nhật phần mềm hệ thống" được chọn trong FIA_X509_EXT.2.1, thì phải bao gồm FPT_TUD_EXT.2 trong ST. Việc sử dụng các chứng thư X.509 sẽ không áp dụng nếu chỉ các hash đã công bố được hỗ trợ cho các bản cập nhật tin cậy.

Tính hiệu lực được xác định bằng đường dẫn chứng thư, ngày hết hạn và trạng thái thu hồi theo FIA_X509_EXT.1. Đối với các chứng thư đã hết hạn, tác giả ST sẽ lựa chọn xem chứng thư có được

chấp nhận không hay bị từ chối, hoặc chọn sự lựa chọn còn lại để quản trị viên đưa ra quyết định chấp nhận hay từ chối chứng thư.

B.4 Quản lý an toàn (FMT)

B.4.1 Quản lý các chức năng trong TSF (FMT_MOF)

B.4.1.1 FMT_MOF.1(2)/TrustedUpdate Quản lý hành vi chức năng an toàn

FMT_MOF.1.1(2)/ TrustedUpdate TSF phải giới hạn khả năng cho phép kích hoạt hay vô hiệu hóa các chức năng [*lựa chọn: tự động kiểm tra để cập nhật, tự động cập nhật*] của *quản trị viên an toàn.*

Chú thích áp dụng: FMT_MOF.1(2)/TrustedUpdate chỉ áp dụng được nếu TOE hỗ trợ các bản cập nhật tự động cũng như cho phép kích hoạt và vô hiệu hóa chúng. Kích hoạt và vô hiệu hóa tính năng cập nhật tự động sẽ được giới hạn cho các quản trị viên an toàn.

Phụ lục C

(Quy định)

Các định nghĩa thành phần mở rộng

C.0 Giới thiệu

Phụ lục này bao gồm các định nghĩa về các yêu cầu mở rộng được sử dụng trong PP, bao gồm cả những định nghĩa được sử dụng trong Phụ lục A và Phụ lục B.

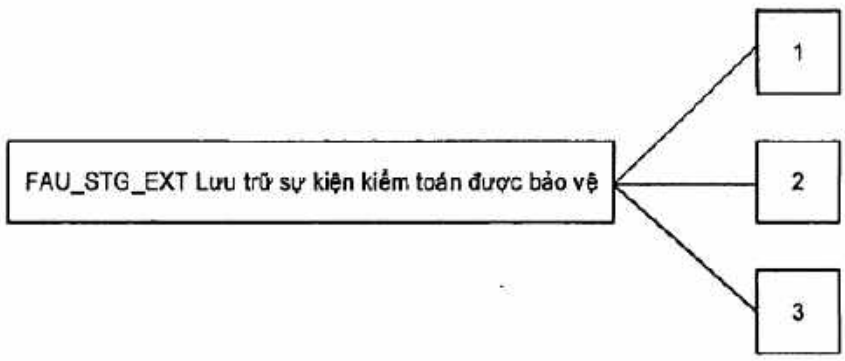
C.1 Kiểm toán an toàn (FAU)

C.1.1 Lưu trữ sự kiện kiểm toán được bảo vệ (FAU_STG_EXT)

Tập hợp các hành vi

Thành phần này định nghĩa các yêu cầu đối với TSF để có thể truyền dữ liệu kiểm toán một cách an toàn giữa TOE và một thực thể IT bên ngoài.

Phân cấp thành phần



FAU_STG_EXT.1 Lưu trữ sự kiện kiểm toán được bảo vệ yêu cầu TSF sử dụng một kênh đáng tin cậy để thực hiện một giao thức an toàn.

FAU_STG_EXT.2 Tính dữ liệu kiểm toán bị mất yêu cầu TSF cung cấp thông tin về hồ sơ kiểm toán bị ảnh hưởng khi nhật ký kiểm toán bị đầy.

FAU_STG_EXT.3 Hiển thị cảnh báo không gian lưu trữ cục bộ yêu cầu TSF tạo cảnh báo trước khi nhật ký kiểm toán bị đầy.

Quản lý: FAU_STG_EXT.1, FAU_STG_EXT.2, FAU_STG_EXT.3

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

a) TSF có khả năng cấu hình chức năng mật mã.

Kiểm toán: FAU_STG_EXT.1, FAU_STG_EXT.2, FAU_STG_EXT.3

Các hành động sau phải kiểm toán được nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Không cần kiểm toán.

C.1.1.1 FAU_ STG_EXT.1 Lưu trữ sự kiện kiểm toán được bảo vệ

Phân cấp: Không có thành phần khác.

Phụ thuộc: FAU_GEN.1 Tạo dữ liệu kiểm toán

FTP_ITC.1 Kênh tin cậy Inter-TSF

FAU_STG_EXT.1.1 TSF phải có thể chuyển dữ liệu kiểm toán được tạo ra cho một thực thể IT bên ngoài bằng cách sử dụng một kênh tin cậy theo FTP_ITC.

Chú thích áp dụng: Để chọn tùy chọn truyền dữ liệu kiểm toán được tạo ra cho một thực thể IT bên ngoài, TOE sẽ dựa vào một máy chủ kiểm toán không phải là TOE để lưu trữ và xem xét hồ sơ kiểm toán. Tính năng lưu trữ các hồ sơ kiểm toán này và khả năng cho phép quản trị viên xem xét các hồ sơ kiểm toán này sẽ do môi trường hoạt động trong trường hợp đó cung cấp.

FAU_STG_EXT.1.2 TSF phải cho phép lưu trữ dữ liệu kiểm toán được tạo ra trên chính TOE.

FAU_STG_EXT.1.3 TSF phải [lựa chọn: *bỏ dữ liệu kiểm toán mới, ghi đè các hồ sơ kiểm toán trước đó theo quy tắc sau: [chỉ định: nguyên tắc ghi đè các hồ sơ kiểm toán trước đó], [chỉ định: hành động khác]]* khi không gian lưu trữ cục bộ cho dữ liệu kiểm toán bị đầy.

Chú thích áp dụng: Máy chủ đăng nhập bên ngoài có thể được sử dụng làm không gian lưu trữ thay thế trong trường hợp không gian lưu trữ cục bộ bị đầy. "Hành động khác" trong trường hợp này có thể được định nghĩa là "gửi dữ liệu kiểm toán mới cho một thực thể IT bên ngoài".

C.1.1.2 FAU_ STG_EXT.2 Tính dữ liệu kiểm toán bị mất

Phân cấp: Không có thành phần khác.

Phụ thuộc: FAU_GEN.1 Tạo dữ liệu kiểm toán

FAU_STG_EXT.1 Lưu trữ dấu vết kiểm toán bên ngoài

FAU_STG_EXT.2.1 TSF phải cung cấp thông tin về số lượng hồ sơ kiểm toán [lựa chọn: *bị bỏ, bị ghi đè, chỉ định: thông tin khác*] trong trường hợp lưu trữ cục bộ bị đầy và TSF thực hiện một trong các hành động được định nghĩa trong FAU_STG_EXT.1.3.

Chú thích áp dụng: Nên chọn tùy chọn này nếu TOE hỗ trợ chức năng này.

Trong trường hợp lưu trữ hồ sơ kiểm toán cục bộ bị xóa bởi quản trị viên, các bộ đếm liên quan đến lựa chọn trong SFR phải được đặt lại về giá trị ban đầu (thường là về 0). Tài liệu hướng dẫn phải bao gồm cả cảnh báo cho quản trị viên về việc mất dữ liệu kiểm toán khi quản trị viên xóa lưu trữ hồ sơ kiểm toán cục bộ.

C.1.1.3 FAU_ STG_EXT.3 Cảnh báo hiển thị cho không gian lưu trữ cục bộ

FAU_STG_EXT.3.1 TSF phải tạo ra một cảnh báo để thông báo cho người dùng trước khi không gian lưu trữ dữ liệu kiểm toán cục bộ được sử dụng hết và/ hoặc TOE sẽ mất dữ liệu kiểm toán do không gian cục bộ không đủ.

Chú thích áp dụng: Nên chọn tùy chọn này nếu TOE tạo ra cảnh báo để thông báo cho người dùng trước khi không gian lưu trữ dữ liệu kiểm toán cục bộ được sử dụng hết. Cách này có thể hữu ích nếu các sự kiện có thể kiểm toán chỉ được lưu trữ trên không gian lưu trữ cục bộ.

Phải đảm bảo thông điệp cảnh báo theo yêu cầu của FAU_STG_EXT.1.3 được truyền đạt tới người dùng. Liên lạc phải được thực hiện thông qua chính nhật ký kiểm toán vì không thể đảm bảo có một phiên hành chính đang hoạt động tại thời điểm xảy ra sự kiện.

C.2 Hỗ trợ mã hóa (FCS)

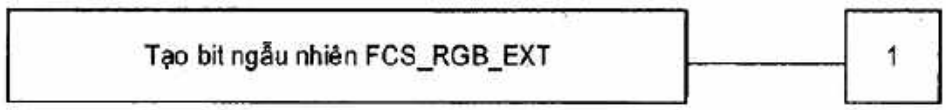
C.2.1 Tạo bit ngẫu nhiên (FCS_RBG_EXT)

C.2.1.1 FCS_ RBG_EXT.1 Tạo bit ngẫu nhiên

Tập hợp các hành vi

Các thành phần trong họ này đưa ra các yêu cầu cho việc tạo bit/số ngẫu nhiên. Đây là một họ mới định nghĩa cho lớp FCS.

Phân cấp thành phần



Tạo bit ngẫu nhiên FCS_RBG_EXT.1 đòi hỏi phải tạo bit ngẫu nhiên theo các tiêu chuẩn đã chọn và được tạo ra bởi một nguồn entropy.

Quản lý: FCS_RBG_EXT.1

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

a) Không có hoạt động quản lý dự kiến

Kiểm toán: FCS_RBG_EXT.1

Các hành động sau cần được kiểm toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Tối thiểu: lỗi quá trình ngẫu nhiên hóa

Phân cấp: Không có thành phần khác.

Phụ thuộc: Không có thành phần khác.

FCS_RBG_EXT.1.1 TSF phải thực hiện tất cả các dịch vụ tạo bit ngẫu nhiên theo tiêu chuẩn ISO/IEC 18031: 2011 bằng cách sử dụng [lựa chọn: *Hash_DRBG (bất kỳ), HMAC_DRBG (bất kỳ), CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 RBG xác định phải được gieo bởi ít nhất một nguồn entropy tích lũy entropy từ [lựa chọn: *[chỉ định: số nguồn dựa trên phần mềm] nguồn nhiễu dựa trên phần mềm, [chỉ định: số nguồn dựa trên phần cứng] nguồn nhiễu dựa trên phần cứng]* với tối thiểu [lựa chọn: *128 bit, 192 bit, 256 bit*] của entropy tối thiểu bằng độ mạnh an toàn lớn nhất, theo tiêu chuẩn ISO/IEC 18031: 2011 Bảng C.1 "Bảng độ mạnh an toàn cho các hàm băm", của các khóa và hàm băm mà nó sẽ tạo ra.

Chú thích áp dụng: Đối với lựa chọn đầu tiên trong FCS_RBG_EXT.1.2, ST chọn ít nhất một trong số các loại nguồn nhiễu. Nếu TOE chứa nhiều nguồn nhiễu cùng loại, tác giả ST sẽ điền vào chỉ định số thích hợp cho từng loại nguồn (ví dụ: 2 nguồn nhiễu dựa trên phần mềm, 1 nguồn nhiễu dựa trên phần cứng). Các tài liệu và hoạt động kiểm toán yêu cầu trong hoạt động đánh giá cho phần tử này nhất thiết phải mô tả từng nguồn được chỉ ra trong ST.

ISO/IEC 18031: 2011 chứa ba phương pháp tạo ra các số ngẫu nhiên khác nhau; mỗi loại này, theo thứ tự, phụ thuộc vào nguyên thủy mã hóa cơ bản (các hàm băm/mật mã). Tác giả ST sẽ chọn hàm được sử dụng, và bao gồm các nguyên mẫu mã hóa cơ bản được sử dụng trong yêu cầu. Mặc dù các hàm băm đã xác định (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) là được phép đối với Hash_DRBG hoặc HMAC_DRBG, chỉ các triển khai dựa trên AES cho CTR_DRBG mới được phép.

C.2.2 Giao thức mã hóa (Mở rộng – FCS_HTTPS_EXT, FCS_ IPSEC_EXT, FCS_SSHC_EXT, FCS_SSHS_EXT, FCS_TLSC_EXT, FCS_TLSS_EXT)

C.2.2.1 HTTPS_EXT.1 Giao thức HTTPS

Tập hợp các hành vi

Các thành phần trong họ này xác định các yêu cầu để bảo vệ các phiên quản lý từ xa giữa TOE và quản trị viên an toàn. Họ này mô tả cách HTTPS sẽ được thực hiện. Đây là một họ mới được xác định cho lớp FCS.

Phân cấp thành phần

Giao thức FCS_HTTPS_EXT HTTPS	1

FCS_HTTPS_EXT.1 HTTPS yêu cầu HTTPS được thực hiện theo RFC 2818 và hỗ trợ TLS.

Quản lý: FCS_HTTPS_EXT.1

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

a) Không có hoạt động quản lý nào dự kiến.

Kiểm toán: FCS_HTTPS_EXT.1

Các hành động sau cần được kiểm toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Không có sự kiện kiểm toán nào được dự kiến.

Phân cấp: Không có thành phần khác.

Phụ thuộc: FCS_TLS_EXT.1 Giao thức TLS.

FCS_HTTPS_EXT.1.1 TSF phải thực hiện giao thức HTTPS tuân thủ RFC 2818.

FCS_HTTPS_EXT.1.2 TSF phải thực hiện giao thức HTTPS sử dụng TLS.

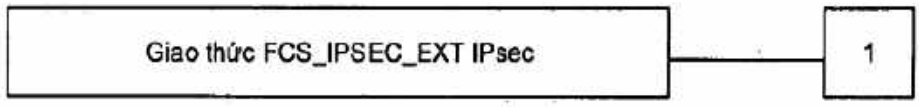
FCS_HTTPS_EXT.1.3 TSF phải [lựa chọn: *không thiết lập kết nối, yêu cầu ủy quyền để thiết lập kết nối, [chỉ định: hành động khác]]* nếu chứng thư ngang hàng được coi là không hợp lệ.

C.2.2.2 FCS_IPSEC_EXT.1 Giao thức IPsec

Tập hợp các hành vi

Các thành phần trong họ này đáp ứng yêu cầu bảo vệ truyền thông bằng cách sử dụng IPsec.

Phân cấp thành phần



FCS_IPSEC_EXT.1 IPsec yêu cầu IPsec được thực hiện như đã quy định.

Quản lý: FCS_IPSEC_EXT.1

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

a) Duy trì cấu hình thời gian sử dụng SA

Kiểm toán: FCS_IPSEC_EXT.1

Các hành động sau cần được kiểm toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Quyết định các gói mạng DISCARD, BYPASS, PROTECT được xử lý bởi TOE.

b) Không thiết lập IPsec SA

c) Thiết lập IPsec SA

d) Chấm dứt IPsec SA

e) Đàm phán "xuống" từ IKEv2 sang IKEv1.

Phân cấp: Không có thành phần khác.

Phụ thuộc: FCS_CKM.1 Tạo khóa mã hóa

FCS_CKM.2 Thiết lập khóa mã hóa

FCS_COP.1(1) Hành động mật mã hóa (Mã hóa/giải mã AES)

FCS_COP.1(2) Hành động mã xóa (Xác thực chữ ký)

FCS_COP.1(3) Hành động mã hóa (Thuật toán băm)

FCS_RBG_EXT.1 Tạo bit ngẫu nhiên

FCS_IPSEC_EXT.1.1 TSF phải thực hiện kiến trúc IPsec theo quy định trong RFC 4301.

Chú thích áp dụng: RFC 4301 yêu cầu thực hiện IPsec để bảo vệ lưu lượng IP thông qua việc sử dụng Cơ sở dữ liệu Chính sách An toàn (SPD). SPD được sử dụng để xác định cách các gói tin IP được xử lý: BẢO VỆ gói tin (ví dụ, mã hóa gói tin), BỎ QUA các dịch vụ IPsec (ví dụ, không mã hóa), hoặc HỦY BỎ gói tin (ví dụ, thả gói tin). SPD có thể được thực hiện bằng nhiều cách khác nhau, bao gồm các danh sách kiểm soát truy cập router, bộ quy tắc tường lửa, SPD "truyền thống"... Dù chi tiết thực hiện như thế nào thì có một khái niệm về "quy tắc" theo đó một gói tin được đối sánh "khớp" thì sẽ có một hành động kết quả diễn ra.

Mặc dù phải có một phương pháp để đặt ra các quy tắc, một cách tiếp cận chung để đặt ra quy tắc là không bắt buộc, miễn là SPD có thể phân biệt các gói tin IP và áp dụng các quy tắc tương ứng. Có thể có nhiều SPD (một cái cho từng giao diện mạng), nhưng điều này là không bắt buộc.

FCS_IPSEC_EXT.1.2 TSF phải có một mục nhập danh nghĩa, cuối cùng trong SPD dành cho những gói đã đối sánh không khớp và loại bỏ những gói này.

FCS_IPSEC_EXT.1.3 TSF phải thực hiện chế độ vận chuyển và [lựa chọn: *chế độ đường hầm, không có chế độ khác*].

FCS_IPSEC_EXT.1.4 TSF phải thực hiện giao thức IPsec ESP theo định nghĩa của RFC 4303 sử dụng các thuật toán mật mã AES-CBC-128, AES-CBC-256 (cả hai được xác định bởi RFC 3602) và [lựa chọn: *AES-GCM-128 (quy định tại RFC 4106), AES-GCM-256 (quy định tại RFC 4106), không có các thuật toán khác*] cùng với một HMAC dựa trên SHA.

FCS_IPSEC_EXT.1.5 TSF phải thực hiện giao thức: [lựa chọn:

- *IKEv1, sử dụng chế độ chính cho các trao đổi trong Giai đoạn 1, như được định nghĩa trong các RFC 2407, 2408, 2409, RFC 4109, [lựa chọn: không có RFC khác cho số thứ tự mở rộng, RFC 4304 cho số thứ tự mở rộng] và [lựa chọn: không có RFC khác cho hàm băm, RFC 4868 cho hàm băm];*
- *IKEv2 như được định nghĩa trong RFC 5996 [lựa chọn: không hỗ trợ giao thoa NAT, với sự hỗ trợ bắt buộc cho giao thoa NAT như quy định trong RFC 5996, điều 2.23)], và [lựa chọn: không có RFC cho các hàm băm, RFC 4868 cho các hàm băm]].*

FCS_IPSEC_EXT.1.6 TSF phải đảm bảo tải trọng mã hóa trong giao thức [lựa chọn: *IKEv1, IKEv2*] sử dụng các thuật toán mật mã AES-CBC-128, AES-CBC-256 như đã nêu trong RFC 3602 và [lựa chọn: *AES-GCM-128, AES-GCM-256 như được xác định trong RFC 5282, không có thuật toán khác*].

Chú thích áp dụng: Chỉ có thể chọn AES-GCM-128 và AES-GCM-256 nếu IKEv2 cũng được chọn, vì không có RFC xác định AES-GCM cho IKEv1.

FCS_IPSEC_EXT.1.7 *TSF phải đảm bảo rằng [lựa chọn:*

- *Thời gian sử dụng SA IKEv1 trong Giai đoạn 1 có thể được cấu hình bởi một quản trị viên an toàn dựa trên [lựa chọn:*
    - *số byte;*
    - *khoảng thời gian, trong đó các giá trị thời gian có thể được cấu hình trong [chỉ định: số nguyên bao gồm 24] giờ;*

    ];
- *Thời gian sử dụng SA IKEv2 có thể được cấu hình bởi một quản trị viên an toàn dựa trên [lựa chọn:*
    - *số byte;*
    - *khoảng thời gian, trong đó các giá trị thời gian có thể được cấu hình trong [phép: số nguyên bao gồm 24] giờ*

    ]

].

Chú thích áp dụng: Tác giả ST chọn yêu cầu IKEv1 hoặc yêu cầu IKEv2 (hoặc cả hai, tùy thuộc vào sự lựa chọn trong FCS_IPSEC_EXT.1.5). Tác giả ST chọn thời gian sử dụng dựa theo dung lượng hoặc thời gian sử dụng dựa trên thời gian (hoặc kết hợp cả hai). Yêu cầu này phải được thực hiện bằng cách cung cấp thời gian sử dụng có thể được cấu hình bởi quản trị viên an toàn (với hướng dẫn thích hợp trong các tài liệu được AGD_OPE ủy quyền). Các giới hạn được lập trình cứng không đáp ứng được yêu cầu này. Nhìn chung, hướng dẫn để thiết lập các thông số của việc thực hiện, bao gồm cả thời gian sử dụng của các SA, nên được đưa vào tài liệu hướng dẫn tạo ra cho AGD_OPE.

FCS_IPSEC_EXT.1.8 *TSF phải đảm bảo rằng [lựa chọn:*

- *Thời gian sử dụng SA IKEv1 trong giai đoạn 2 có thể được cấu hình bởi quản trị viên an toàn dựa trên [lựa chọn:*
    - *số byte;*
    - *khoảng thời gian, trong đó các giá trị thời gian có thể được cấu hình trong [chỉ định: số nguyên bao gồm 8] giờ;*

];

- *Thời gian sử dụng của Child SA IKEv2 có thể được cấu hình bởi một quản trị viên an toàn dựa trên [lựa chọn:*
  - *số byte;*
  - *khoảng thời gian, trong đó các giá trị thời gian có thể được cấu hình trong [chỉ định: số nguyên bao gồm 8] giờ;*

  ]

].

Chú thích áp dụng: Tác giả ST chọn yêu cầu IKEv1 hoặc yêu cầu IKEv2 (hoặc cả hai, tùy thuộc vào sự lựa chọn trong FCS_IPSEC_EXT.1.5). Tác giả ST chọn thời gian sử dụng dựa theo dung lượng hoặc thời gian sử dụng dựa trên thời gian (hoặc kết hợp cả hai). Yêu cầu này phải được thực hiện bằng cách cung cấp thời gian sử dụng có thể được cấu hình bởi quản trị viên an toàn (với hướng dẫn thích hợp trong các tài liệu được AGD_OPE ủy quyền). Các giới hạn được lập trình cứng không đáp ứng được yêu cầu này. Nhìn chung, hướng dẫn để thiết lập các thông số của việc thực hiện, bao gồm cả thời gian sử dụng của các SA, nên được đưa vào tài liệu hướng dẫn tạo ra cho AGD_OPE.

FCS_IPSEC_EXT.1.9 TSF phải tạo ra giá trị bí mật x được sử dụng trong trao đổi khóa IKE Diffie-Hellman ("x" trong gx mod g) bằng cách sử dụng bộ tạo bit ngẫu nhiên được chỉ định trong FCS_RBG_EXT.1 và có độ dài ít nhất là [chỉ định: *(một hoặc nhiều) số bit ít nhất gấp đôi độ an toàn của nhóm Diffie-Hellman đã thương lượng]* bit.

Chú thích áp dụng: Đối với nhóm DH nhóm 19 và 20, giá trị "x" là số nhân điểm cho điểm phát của G.

Vì việc thực hiện có thể cho phép các nhóm Diffie-Hellman khác nhau được đàm phán để sử dụng trong việc thiết lập các SA, chỉ định trong FCS_IPSEC_EXT.1.9 có thể chứa nhiều giá trị. Đối với mỗi nhóm DH được hỗ trợ, Tác giả ST tham vấn Bảng 2 trong NIST SP 800-57 "Khuyến nghị về quản lý khóa – Phần 1: Tổng quát" để xác định độ mạnh an toàn ("các bit an toàn") liên quan đến nhóm DH. Mỗi giá trị duy nhất sau đó được sử dụng để điền vào chỉ định cho phần tử này. Ví dụ, giả sử việc thực hiện hỗ trợ nhóm DH 14 (2048-bit MODP) và nhóm 20 (ECDH sử dụng đường cong NIST P-384). Từ Bảng 2, giá trị các bit an toàn cho nhóm 14 là 112, và nhóm 20 là 192.

FCS_IPSEC_EXT.1.10 TSF phải tạo ra các nonce được sử dụng trong trao đổi [lựa chọn: *IKEv1, IKEv2*] có chiều dài [lựa chọn:

- *[chỉ định: độ mạnh an toàn liên quan đến nhóm Diffie-Hellman đã đàm phán];*
- *Tối thiểu có kích thước 128 bit và ít nhất một nửa kích thước đầu ra của hàm giả băm ngẫu nhiên đã được đàm phán (PRF)*

].

Chú thích áp dụng: Tác giả ST phải chọn tùy chọn thứ hai cho các chiều dài nonce nếu IKEv2 cũng được chọn (vì điều này được yêu cầu trong RFC 5996). Tác giả ST có thể chọn một trong hai tùy chọn cho IKEv1.

Đối với tùy chọn đầu tiên cho các chiều dài nonce, vì việc triển khai có thể cho phép các nhóm Diffie-Hellman khác được thương lượng để sử dụng trong việc thiết lập các SA, chỉ định trong FCS_IPSEC_EXT.1.10 có thể chứa nhiều giá trị. Đối với mỗi nhóm DH được hỗ trợ, Tác giả ST tham khảo Bảng 2 trong NIST SP 800-57 "Khuyến nghị về quản lý khóa - Phần 1: Tổng quát" để xác định độ mạnh an toàn ("các bit an toàn") liên quan đến nhóm DH. Mỗi giá trị duy nhất sau đó được sử dụng để điền vào chỉ định cho phần tử này. Ví dụ, giả sử việc thực hiện hỗ trợ nhóm DH 14 (2048-bit MODP) và nhóm 20 (ECDH sử dụng đường cong NIST P-384). Từ Bảng 2, giá trị các bit an toàn cho nhóm 14 là 112, và nhóm 20 là 192.

Bởi vì tại thời điểm này có thể được trao đổi trước khi nhóm DH được đàm phán, nonce sử dụng nên được đủ lớn để hỗ trợ tất cả các đề xuất TOE-lựa chọn trong trao đổi.

FCS_IPSEC_EXT.1.11 TSF phải đảm bảo rằng tất cả các giao thức IKE thực hiện DH Nhóm 14 (2048-bit MODP), và [lựa chọn: *19 (ECP 256 bit ngẫu nhiên), 5 (1536-bit MODP), 24 (2048-bit MODP với POS 256 bit), 20 (ECP 384-bit ngẫu nhiên), [chỉ định: nhóm DH khác được thực hiện bởi TOE], không có nhóm DH nào khác*].

FCS_IPSEC_EXT.1.12 TSF phải có thể để đảm bảo theo mặc định rằng độ mạnh của thuật toán đối xứng (về số bit trong khóa) đàm phán để bảo vệ [lựa chọn: IKEv1 Giai đoạn 1, giao thức IKEv2 IKE_SA] kết nối lớn hơn hoặc bằng sức mạnh của thuật toán đối xứng (về số lượng bit trong khóa) được thương lượng để bảo vệ kết nối [lựa chọn: *IKEv1 Giai đoạn 2, IKEv2 CHILD_SA*].

Chú thích áp dụng: Tác giả ST chọn một hoặc cả hai lựa chọn IKE dựa trên những gì được thực hiện bởi TOE. Mặc dù cấu hình mặc định trong cấu hình được đánh giá ("ngoài phạm vi" hoặc hướng dẫn cấu hình trong tài liệu AGD) có thể được cấu hình, nhưng phải cho phép chức năng này.

FCS_IPSEC_EXT.1.13 TSF phải đảm bảo rằng tất cả các giao thức IKE thực hiện xác thực ngang hàng bằng cách sử dụng [lựa chọn: *RSA, ECDSA*] dùng các chứng thư X.509v3 phù hợp với RFC 4945 và [lựa chọn: *Khóa chia sẻ trước, không có phương pháp nào khác*].

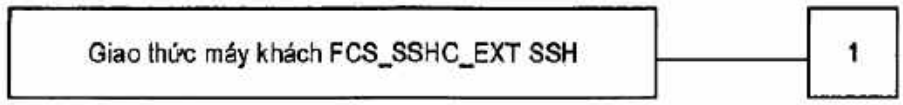
FCS_IPSEC_EXT.1.14 TSF chỉ thiết lập một kênh đáng tin cậy cho các mạng ngang hàng có chứng thư hợp lệ.

C.2.2.3 FCS_SSHC_EXT.1 Giao thức máy khách SSH

Tập hợp các hành vi

Thành phần trong họ này đề cập khả năng cho một máy khách sử dụng SSH để bảo vệ dữ liệu giữa máy khách và máy chủ sử dụng giao thức SSH.

Phân cấp thành phần



Giao thức máy khách FCS_SSHC_EXT.1 SSH yêu cầu phía máy khách của SSH được thực hiện theo quy định.

Quản lý: FCS_SSHC_EXT.1

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

a) Không có hoạt động quản lý nào dự kiến.

Kiểm toán: FCS_SSHC_EXT.1

Các hành động sau cần được kiểm toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Không thiết lập SSH.

b) Thiết lập phiên SSH

c) Chấm dứt phiên SSH

FCS_SSHC_EXT.1 Máy khách SSH yêu cầu các khía cạnh của SSH để triển khai cụ thể.

Phân cấp:	Không có thành phần khác
Phụ thuộc:	FCS_COP.1(1) Hành động mã hóa (Mã hóa và giải mã dữ liệu AES)
	FCS_COP.1(2) Hành động mã hóa (Xác thực chữ ký)
	FCS_COP.1(3) Hành động mã hóa (Thuật toán băm)

FCS_SSHC_EXT.1.1 TSF phải thực hiện giao thức SSH tuân thủ các RFC 4251, 4252, 4253, 4254, và [lựa chọn: *5647, 5656, 6187, 6668, không có các RFC khác*].

Chú thích áp dụng: Tác giả ST chọn các RFC bổ sung mà đã có yêu cầu tuân thủ. Lưu ý rằng chúng cần phải nhất quán với các lựa chọn trong các phần tử sau của thành phần này (ví dụ, thuật toán mật mã cho phép). RFC 4253 chỉ ra rằng một số thuật toán mật mã nhất định là "BẮT BUỘC". Điều này có nghĩa là việc triển khai phải bao gồm hỗ trợ chứ không phải là các thuật toán phải được kích hoạt để sử dụng. Đảm bảo rằng các thuật toán được chỉ định là "BẮT BUỘC" nhưng không được liệt kê trong các phần tử sau của thành phần này được thực hiện nằm ngoài phạm vi của hoạt động đảm bảo cho yêu cầu này.

FCS_SSHC_EXT.1.2 TSF phải đảm bảo rằng việc thực hiện giao thức SSH hỗ trợ các phương pháp xác thực sau đây như được mô tả trong RFC 4252: dựa trên khóa công khai, dựa trên mật khẩu.

FCS_SSHC_EXT.1.3 TSF phải đảm bảo rằng, như được mô tả trong RFC 4253, các gói tin lớn hơn [chỉ định: *số lượng byte*] byte trong kết nối vận chuyển SSH bị rớt.

Chú thích áp dụng: RFC 4253 cung cấp cho việc chấp nhận "các gói tin lớn" với báo trước rằng các gói tin nên có "chiều dài hợp lý" hoặc bị rớt. Chỉ định phải được điền bởi tác giả ST với kích thước gói tin tối đa được chấp nhận, do đó xác định "chiều dài hợp lý" cho TOE.

FCS_SSHC_EXT.1.4 TSF phải đảm bảo rằng việc thực hiện vận chuyển SSH sử dụng các thuật toán mã hóa sau và từ chối tất cả các thuật toán mã hóa khác: [chỉ định: *Danh sách các thuật toán mã hóa*].

FCS_SSHC_EXT.1.5 TSF phải đảm bảo rằng việc triển khai vận chuyển SSH sử dụng các thuật toán khóa công khai là thuật toán khóa công khai của nó và loại bỏ tất cả các thuật toán khóa công khai khác.

FCS_SSHC_EXT.1.6 TSF phải đảm bảo rằng việc triển khai vận chuyển SSH sử dụng các thuật toán MAC toàn vẹn dữ liệu như là thuật toán MAC toàn vẹn dữ liệu của nó và từ chối tất cả các thuật toán MAC khác.

FCS_SSHC_EXT.1.7 TSF phải đảm bảo rằng [chỉ định: *Danh sách các phương pháp trao đổi khóa*] là các phương pháp trao đổi khóa duy nhất được sử dụng cho giao thức SSH.

FCS_SSHC_EXT.1.8 TSF phải đảm bảo rằng kết nối SSH được ghi lại sau khi không có hơn 2 ^ 28 gói tin đã được truyền bằng khóa đó.

FCS_SSHC_EXT.1.9 TSF phải đảm bảo rằng máy khách SSH xác thực định danh của máy chủ SSH bằng cách sử dụng cơ sở dữ liệu cục bộ liên kết mỗi tên máy chủ với khóa công khai tương ứng hoặc [lựa chọn: *một danh sách các cơ quan chứng nhận đáng tin cậy, không có các phương pháp khác*] như được mô tả trong RFC 4251 điều 4.1.

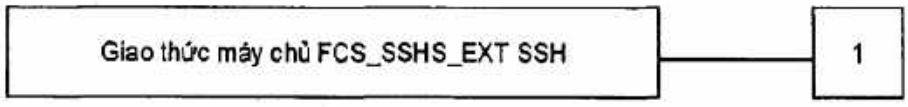
Chú thích áp dụng: Danh sách các cơ quan chứng nhận đáng tin cậy chỉ có thể được chọn nếu x509v3-ecdsa-sha2-nistp256 hoặc x509v3-ecdsa-sha2-nistp384 được chỉ định trong FCS_SSHC_EXT.1.5.

C.2.2.4 FCS_SSHS_EXT.1 Giao thức máy chủ SSH

Tập hợp các hành vi

Thành phần trong họ này đề cập khả năng cho một máy chủ cung cấp SSH để bảo vệ dữ liệu giữa máy khách và máy chủ sử dụng giao thức SSH.

Phân cấp thành phần



Giao thức máy chủ FCS_SSHS_EXT.1 SSH yêu cầu phía máy chủ của SSH được thực hiện như đã quy định.

Quản lý: FCS_SSHS_EXT.1

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

a) Không có hoạt động quản lý nào dự kiến.

Kiểm toán: FCS_SSHS_EXT.1

Các hành động sau cần được toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Không thiết lập SSH.

b) Thiết lập phiên SSH

c) Chấm dứt phiên SSH

Phân cấp:	Không có thành phần khác
Phụ thuộc:	FCS_COP.1(1) Hành động mã hóa (Mã hóa/giải mã dữ liệu AES)
	FCS_COP.1(2) Hành động mã hóa (Xác thực chữ ký)
	FCS_COP.1(3) Hành động mã hóa (Thuật toán băm)

FCS_SSHS_EXT.1.1 TSF phải thực hiện giao thức SSH tuân thủ các RFC 4251, 4252, 4253, 4254, và [lựa chọn: *5647, 5656, 6187, 6668, không có các RFC khác*].

Chú thích áp dụng: Tác giả ST chọn các RFC bổ sung mà đã có yêu cầu tuân thủ. Lưu ý rằng chúng cần phải nhất quán với các lựa chọn trong các phần tử sau của thành phần này (ví dụ, thuật toán mật mã cho phép). RFC 4253 chỉ ra rằng một số thuật toán mật mã nhất định là "BẮT BUỘC". Điều này có nghĩa là việc triển khai phải bao gồm hỗ trợ chứ không phải là các thuật toán phải được kích hoạt để sử dụng. Đảm bảo rằng các thuật toán được chỉ định là "BẮT BUỘC" nhưng không được liệt kê trong các phần tử sau của thành phần này được thực hiện nằm ngoài phạm vi của hoạt động đảm bảo cho yêu cầu này.

FCS_SSHS_EXT.1.2 TSF phải đảm bảo rằng việc thực hiện giao thức SSH hỗ trợ các phương pháp xác thực sau đây như mô tả trong RFC 4252: dựa trên khóa công khai, dựa trên mật khẩu.

FCS_SSHS_EXT.1.3 TSF phải đảm bảo rằng, như được mô tả trong RFC 4253, các gói tin lớn hơn [chỉ định: *số lượng byte*] byte trong kết nối truyền thông SSH bị rớt.

Chú thích áp dụng: RFC 4253 cung cấp cho việc chấp nhận "các gói tin lớn" với báo trước rằng các gói tin nên có "chiều dài hợp lý" hoặc bị rớt. Chỉ định phải được điền bởi Tác giả ST với kích thước gói tin tối đa được chấp nhận, do đó xác định "chiều dài hợp lý" cho TOE.

FCS_SSHS_EXT.1.4 TSF phải đảm bảo rằng việc triển khai vận chuyển SSH sử dụng các thuật toán mã hóa sau và từ chối tất cả các thuật toán mã hóa khác: [chỉ định: *thuật toán mã hóa*].

FCS_SSHS_EXT.1.5 TSF phải đảm bảo rằng việc thực hiện vận chuyển SSH sử dụng [chỉ định: *danh sách thuật toán khóa công khai*] thuật toán khóa công khai và làm mất tất cả các thuật toán khóa công khai khác.

FCS_SSHS_EXT.1.6 TSF phải đảm bảo rằng việc thực hiện vận chuyển SSH sử dụng [chỉ định: *danh sách thuật toán MAC*] thuật toán MAC của nó và loại bỏ tất cả các thuật toán MAC khác.

FCS_SSHS_EXT.1.7 TSF phải đảm bảo rằng [chỉ định: *Danh sách các phương pháp trao đổi khóa*] là các phương pháp trao đổi khóa duy nhất được sử dụng cho giao thức SSH.

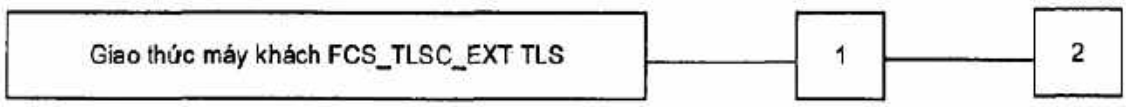
FCS_SSHS_EXT.1.8 TSF phải đảm bảo rằng kết nối SSH được ghi lại sau khi không quá 2 ^ 28 gói được truyền bằng khóa đó.

C.2.2.5 FCS_TLSC_EXT Giao thức máy khách TLS

Tập hợp các hành vi

Thành phần trong họ này đề cập khả năng cho một máy khách sử dụng TLS để bảo vệ dữ liệu giữa máy khách và máy chủ sử dụng giao thức TLS.

Phân cấp thành phần



Giao thức máy khách FCS_TLSC_EXT.1 TLS yêu cầu bên máy khách của TLS được thực hiện như quy định.

Giao thức máy khách FCS_TLSC_EXT.2 TLS yêu cầu phía máy khách thực hiện TLS bao gồm xác thực lẫn nhau.

Quản lý: FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

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

a) Không có hoạt động quản lý nào dự kiến.

Kiểm toán: FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

Các hành động sau cần được kiểm toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Không thiết lập phiên TLS.

b) Thiết lập phiên TLS

c) Chấm dứt phiên TLS

Phân cấp:	Không có thành phần khác
Phụ thuộc:	FCS_COP.1(1) Hành động mã hóa (Mã hóa/giải mã dữ liệu AES)
	FCS_COP.1(2) Hành động mã hóa (Xác thực chữ ký)
	FCS_COP.1(3) Hành động mã hóa (Thuật toán băm)

FCS_RBG_EXT.1 Tạo bit ngẫu nhiên

FCS_TLSC_EXT.1.1 TSF phải thực hiện [lựa chọn: *TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] hỗ trợ ciphersuites sau:

- *- Ciphersuites bắt buộc:*
    - *[Chỉ định: Danh sách ciphersuites bắt buộc và tham chiếu đến RFC trong đó mỗi loại được xác định]*
- *[lựa chọn: Ciphersuites tùy chọn:*
    - *[Chỉ định: Danh sách tùy chọn mã và tham chiếu đến RFC trong đó mỗi loại đều được xác định]*
    - *không có ciphersuite khác]].*

Chú thích áp dụng: Các ciphersuites được kiểm tra trong cấu hình đánh giá được giới hạn bởi yêu cầu này. Lưu ý rằng TLS_RSA_WITH_AES_128_CBC_SHA là bắt buộc để đảm bảo tuân thủ RFC 5246.

FCS_TLSC_EXT.1.2 TSF phải xác minh rằng các định danh được trình bày phù hợp với định danh tham chiếu theo RFC 6125.

Chú thích áp dụng: Các quy tắc xác minh danh tính được mô tả trong Điều 6 của RFC 6125. Từ định dạng tham chiếu được thiết lập bởi người dùng (ví dụ như nhập URL vào một trình duyệt web hoặc nhấp vào một liên kết) bằng cách cấu hình (ví dụ như cấu hình tên của máy chủ thư hoặc máy chủ xác thực), hoặc bởi một ứng dụng (ví dụ như một tham số của một API) tùy thuộc vào dịch vụ ứng dụng. Dựa vào tên miền nguồn và loại dịch vụ ứng dụng (ví dụ HTTP, SIP, LDAP), máy khách thiết lập tất cả các định danh tham chiếu được chấp nhận, chẳng hạn như tên chung cho trường Tên chủ thể của chứng thư và một (trường hợp không nhạy cảm) Tên DNS, tên URI và tên dịch vụ cho trường Tên Thay thế Chủ đề. Sau đó máy khách so sánh danh sách này của tất cả các định danh tham chiếu có thể chấp nhận được với các định danh được trình bày trong chứng thư của máy chủ TLS.

FCS_TLSC_EXT.1.3 TSF chỉ thiết lập một kênh đáng tin cậy nếu chứng thư mạng ngang hàng là hợp lệ.

Chú thích áp dụng: Tính hợp lệ được xác định bởi xác minh định danh, đường dẫn chứng thư, ngày hết hạn và trạng thái thu hồi theo RFC 5280.

FCS_TLSC_EXT.1.4 TSF phải giới thiệu Mở rộng các đường cong Elliptic được hỗ trợ trong Clien Hello với các đường cong NIST sau: [chỉ định: *Danh sách các đường cong được hỗ trợ bao gồm một tùy chọn cho 'Không'*].

Chú thích áp dụng: Nếu đã được chọn ciphersuites với đường cong elliptic trong FCS_TLSC_EXT.1.1, cần phải có một hoặc nhiều đường cong. Nếu không có ciphersuites với đường cong elliptic được chọn trong FCS_TLS_EXT.1.1, thì "Không" nên được chọn.

Yêu cầu này giới hạn các đường cong elliptic cho phép xác thực và thỏa thuận khóa với các đường cong NIST từ FCS_COP.1 (2) và FCS_CKM.1 và FCS_CKM.2. Phần mở rộng này là bắt buộc đối với các máy khách hỗ trợ đường cong elliptic ciphersuite.

Phân cấp:	Giao thức máy khách FCS_TLSC_EXT.1 TLS
Phụ thuộc:	FCS_COP.1(1) Hành động mã hóa (Mã hóa/giải mã dữ liệu AES)
	FCS_COP.1(2) Hành động mã hóa (Xác thực chữ ký)
	FCS_COP.1(3) Hành động mã hóa (Thuật toán băm)
	FCS_RBG_EXT.1 Tạo bit ngẫu nhiên

FCS_TLSC_EXT.2.1 TSF phải thực hiện [lựa chọn: TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] hỗ trợ các thuật ngữ ciphersuites sau:

- *Ciphersuites bắt buộc:*
    - *[chỉ định: Danh sách ciphersuites bắt buộc và tham chiếu đến RFC trong đó mỗi được xác định]*
- *[lựa chọn: Ciphersuites tùy chọn:*
    - *[chỉ định: Danh sách tùy chọn mã và tham chiếu đến RFC trong đó mỗi loại đều được xác định]*
    - *không có ciphersuite khác]].*

Chú thích áp dụng: Các ciphersuites được kiểm tra trong cấu hình đánh giá được giới hạn bởi yêu cầu này. Lưu ý rằng TLS_RSA_WITH_AES_128_CBC_SHA là bắt buộc để đảm bảo tuân thủ RFC 5246.

FCS_TLSC_EXT.2.2 TSF phải xác minh rằng các định danh được trình bày phù hợp với tù định danh tham chiếu theo RFC 6125.

Chú thích áp dụng: Các quy tắc xác minh xác định được mô tả trong Điều 6 của RFC 6125. Định danh tham chiếu được thiết lập bởi người dùng (ví dụ như nhập URL vào một trình duyệt web hoặc nhấp vào một liên kết) bằng cách cấu hình (ví dụ như cấu hình tên của máy chủ thư hoặc máy chủ xác thực), hoặc bởi một ứng dụng (ví dụ như một tham số của một API) tùy thuộc vào dịch vụ ứng dụng. Dựa vào tên miền nguồn và loại dịch vụ ứng dụng (ví dụ HTTP, SIP, LDAP), khách hàng thiết lập tất cả các định danh tham chiếu được chấp nhận, chẳng hạn như tên chung cho trường Tên chủ thể của chứng thư và một (trường hợp không nhạy cảm) Tên DNS, Tên URI và Tên dịch vụ cho trường Tên thay thế Chủ thể. Sau đó khách hàng so sánh danh sách này của tất cả các định danh tham chiếu có thể chấp nhận được với các định danh được trình bày trong chứng thư của máy chủ TLS.

FCS_TLSC_EXT.2.3 TSF chỉ thiết lập một kênh đáng tin cậy nếu chứng thư mạng ngang hàng là hợp lệ.

Chú thích áp dụng: Tính hợp lệ được xác định bởi xác minh định danh, đường dẫn chứng thư, ngày hết hạn và trạng thái thu hồi theo RFC 5280.

FCS_TLSC_EXT.2.4 TSF phải trình bày Mở rộng các đường cong Elliptic được hỗ trợ trong Client Hello với các đường cong NIST sau: [Chỉ định: *Danh sách các đường cong được hỗ trợ bao gồm một tùy chọn cho "Không"*].

FCS_TLSC_EXT.2.5 TSF **phải hỗ trợ xác thực lẫn nhau bằng các chứng thư X.509v3.**

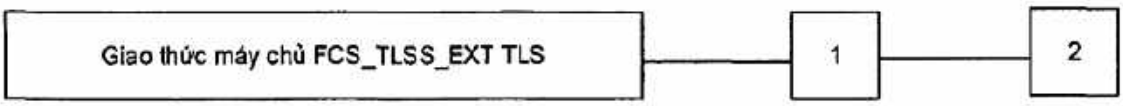
Chú thích áp dụng: Việc sử dụng chứng thư X.509v3 cho TLS được đề cập trong FIA_X509_EXT.2.1. Yêu cầu này cho biết thêm rằng việc sử dụng này phải bao gồm máy khách phải có khả năng trình chứng thư cho máy chủ TLS để chứng thực lẫn nhau TLS.

C.2.2.6 FCS_TLSS_EXT Giao thức máy chủ TLS

Tập hợp các hành vi

Thành phần trong họ này đề cập khả năng cho một máy chủ sử dụng TLS để bảo vệ dữ liệu giữa máy khách và máy chủ sử dụng giao thức TLS.

Phân cấp thành phần



Giao thức máy chủ FCS_TLSS_EXT.1 TLS đòi hỏi phía máy chủ của TLS được thực hiện như đã chỉ định.

FCS_TLSS_EXT.2: Máy chủ TLS yêu cầu xác thực lẫn nhau được bao gồm trong việc triển khai TLS.

Quản lý: FCS_TLSS_EXT.1, FCS_TLSS_EXT.2

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

a) Không có hoạt động quản lý nào dự kiến.

Kiểm toán: FCS_TLSS_EXT.1, FCS_TLSS_EXT.2

Các hành động sau cần được kiểm tra nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Không thiết lập phiên TLS.

b) Thiết lập phiên TLS

c) Chấm dứt phiên TLS

Phân cấp: Không có thành phần khác

Phụ thuộc: FCS_CKM.1 Tạo khóa mã hóa

FCS_COP.1(1) Hành động mã hóa (Mã hóa/giải mã dữ liệu AES)

FCS_COP.1(2) Hành động mã hóa (Xác thực chữ ký)

FCS_COP.1(3) Hành động mã hóa (Thuật toán băm)

FCS_RBG_EXT.1 Tạo bit ngẫu nhiên

FCS_TLSS_EXT.1.1 TSF phải thực hiện [lựa chọn: *TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] hỗ trợ các ciphersuites sau:

- *Ciphersuites bắt buộc:*
    - *[chỉ định: Danh sách ciphersuites bắt buộc và tham chiếu đến RFC trong đó mỗi l oại đều được xác định]*
- *[lựa chọn: Ciphersuites tùy chọn:*
    - *[Chỉ định: Danh sách ciphersuites tùy chọn và tham chiếu đến RFC trong đó mỗi loại đều được xác định]*
    - *không có ciphersuite khác]].*

Chú thích áp dụng: Các ciphersuites được kiểm tra trong cấu hình đánh giá được giới hạn bởi yêu cầu này. Lưu ý rằng TLS_RSA_WITH_AES_128_CBC_SHA là bắt buộc để đảm bảo tuân thủ RFC 5246.

FCS_TLSS_EXT.1.2 TSF phải từ chối các kết nối từ các máy khách yêu cầu SSL 1.0, SSL 2.0, SSL 3.0, TLS 1.0, và [lựa chọn: *TLS 1.1, TLS 1.2, không có*].

Chú thích áp dụng: Bất kỳ phiên bản TLS nào không được chọn trong FCS_TLSS_EXT.1.1 đều phải được chọn ở đây.

FCS_TLSS_EXT.1.3 TSF phải tạo ra các tham số thiết lập quan trọng bằng cách sử dụng RSA với kích thước khóa 2048 bit và [lựa chọn: *3072 bit, 4096 bit, không có kích thước khác*] và [lựa chọn: *[chỉ định: Danh sách các đường cong elliptic]; [Chỉ định: Danh sách các tham số diffie-hellman]*].

Chú thích áp dụng: Các chỉ định sẽ được điền vào dựa trên các chỉ định được thực hiện trong FCS_TLSS_EXT.1.1.

Phân cấp: Giao thức máy chủ FCS_TLSS_EXT.1 TLS

Phụ thuộc: FCS_CKM.1 Tạo khóa mã hóa

FCS_COP.1(1) Hành động mã hóa (Mã hóa/giải mã dữ liệu AES)

FCS_COP.1(2) Hành động mã hóa (Xác thực chữ ký)

FCS_COP.1(3) Hành động mã hóa (Thuật toán băm)

FCS_RBG_EXT.1 Tạo bit ngẫu nhiên

FCS_TLSS_EXT.2.1 TSF phải thực hiện [lựa chọn: *TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] hỗ trợ các ciphersuites sau:

- *Ciphersuites bắt buộc:*
    - *[chỉ định: Danh sách ciphersuites bắt buộc và tham chiếu đến RFC trong đó mỗi loại đều được xác định]*
- *[lựa chọn: Ciphersuites tùy chọn:*
    - *[Chỉ định: Danh sách ciphersuites tùy chọn và tham chiếu đến RFC trong đó mỗi loại đều được xác định]*
    - *không có ciphersuite khác]].*

Chú thích áp dụng: Các ciphersuites được kiểm tra trong cấu hình đánh giá được giới hạn bởi yêu cầu này. Lưu ý rằng TLS_RSA_WITH_AES_128_CBC_SHA là bắt buộc để đảm bảo tuân thủ RFC 5246.

FCS_TLSS_EXT.2.2 TSF phải từ chối các kết nối từ các máy khách yêu cầu SSL 1.0, SSL 2.0, SSL 3.0, TLS 1.0, và [lựa chọn: *TLS 1.1, TLS 1.2, không có*].

Chú thích áp dụng: Nên chọn bất kỳ phiên bản TLS nào không được chọn trong FCS_TLSS_EXT.2.1 tại đây.

FCS_TLSS_EXT.2.3 TSF phải tạo ra các tham số thiết lập quan trọng bằng cách sử dụng RSA với kích thước khóa 2048 bit và [lựa chọn: *3072 bit, 4096 bit, không có kích thước khác*] và [lựa chọn: *[chỉ định: danh sách đường cong elliptic]; [chỉ định: Danh sách các tham số diffie-hellman]*].

Chú thích áp dụng: Các chỉ định sẽ được điền vào dựa trên các chỉ định được thực hiện trong FCS_TLSS_EXT.2.1.

FCS_TLSS_EXT.2.4 TSF phải hỗ trợ xác thực lẫn nhau của các máy khách TLS sử dụng chứng thư X.509v3.

Chú thích áp dụng: Việc sử dụng chứng thư X.509v3 cho TLS được đề cập trong FIA_X509_EXT.2.1. Yêu cầu này bổ sung thêm rằng việc sử dụng này phải bao gồm hỗ trợ cho các chứng thư phía máy khách để xác thực lẫn nhau TLS.

FCS_TLSS_EXT.2.5 TSF phải không thiết lập một kênh tin cậy nếu chứng thư ngang hàng không hợp lệ.

Chú thích áp dụng: Hiệu lực được xác định bởi đường dẫn chứng thư, ngày hết hạn và trạng thái thu hồi theo RFC 5280.

FCS_TLSS_EXT.2.6 TSF phải không thiết lập một kênh đáng tin cậy nếu tên phân biệt (DN) hoặc tên thay thế chủ thể (SAN) có trong một chứng thư không khớp với định danh dự kiến của mạng ngang hàng.

Chú thích áp dụng: Yêu cầu này chỉ áp dụng cho những TOE đang thực hiện TLS được xác thực lẫn nhau (FCS_TLSS_EXT.2.4). Mã định danh peer có thể nằm trong trường Subject hoặc phần mở rộng Subject Alternative Name của chứng thư. Định danh mong muốn có thể được cấu hình, có thể được so sánh với Tên miền, địa chỉ IP, tên người dùng hoặc địa chỉ email được sử dụng bởi mạng ngang hàng, hoặc có thể được chuyển đến một máy chủ thư mục để so sánh.

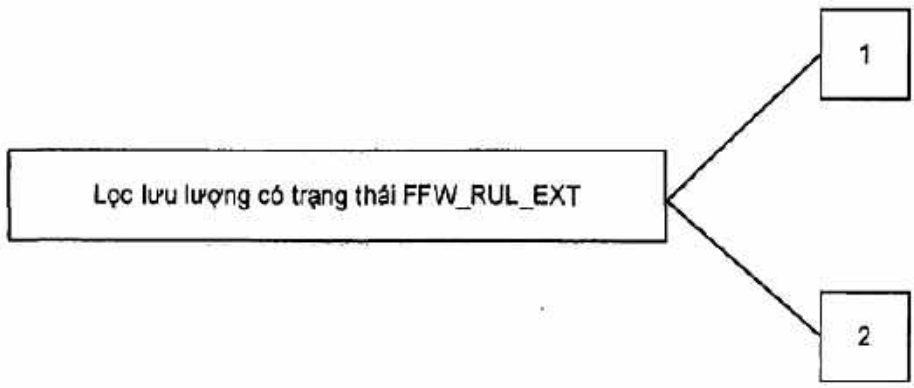
C.3 Tường lửa (FFW)

C.3.1 Tường lửa Lọc lưu lượng có trạng thái (FFW_RUL_EXT)

Tập hợp các hành vi

Yêu cầu này được sử dụng để xác định hành vi của một Tường lửa Lọc lưu lượng có trạng thái. Các giao thức mạng mà TOE có thể lọc, cũng như các thuộc tính có thể được quản trị viên sử dụng để xây dựng một bộ quy tắc được xác định trong thành phần này. Cách thức bộ quy tắc được xử lý (tức là, trình tự) được xác định, cũng như bất kỳ hành vi mặc định được mong đợi của TOE.

Phân cấp thành phần



FFW_RUL_EXT.1 Bộ lọc lưu lượng có trạng thái yêu cầu TOE lọc lưu lượng mạng dựa trên bộ quy tắc được cấu hình bởi một quản trị viên được ủy quyền.

Quản lý: FFW_RUL_EXT.1

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

a) bật/tắt một bộ quy tắc trên một giao diện mạng

b) cấu hình một bộ quy tắc

c) xác định các quy tắc chi phối việc sử dụng các nguồn lực

Kiểm toán: FFW_RUL_EXT.1

Các hành động sau cần được kiểm toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Tối thiểu:

- *Kết quả (tức là, bỏ qua, cho phép) áp dụng một quy tắc trong bộ quy tắc vào một gói mạng*
- *Cấu hình của bộ quy tắc*
- *Chỉ thị các gói dữ liệu đã bị bỏ qua do quá nhiều lưu lượng mạng.*

C.3.1.1 FFW_RUL_EXT.1 Lọc lưu lượng có trạng thái

Phân cấp: Không có thành phần khác

Phụ thuộc: Không

FFW_RUL_EXT.1.1 TSF phải thực hiện Lọc lưu lượng có trạng thái trên các gói tin mạng được xử lý bởi TOE.

FFW_RUL_EXT.1.2 TSF phải cho phép định nghĩa các quy tắc Lọc lưu lượng có trạng thái sử dụng các trường giao thức mạng sau: [chỉ định: *danh sách thuộc tính được hỗ trợ bởi bộ quy tắc*].

FFW_RUL_EXT.1.3 TSF phải cho phép các hoạt động sau được liên kết với các quy tắc Lọc lưu lượng có trạng thái: cho phép hoặc bỏ qua khả năng đăng nhập hoạt động.

FFW_RUL_EXT.1.4 TSF phải cho phép các quy tắc Lọc lưu lượng có trạng thái được gán cho mỗi giao diện mạng riêng biệt.

FFW_RUL_EXT.1.5 TSF phải:

a) chấp nhận một gói tin mạng mà không cần xử lý thêm các quy tắc Lọc lưu lượng có trạng thái nếu nó khớp với một phiên đã được phép thiết lập cho các giao thức sau: [chỉ định: *danh sách các giao thức được hỗ trợ cho trạng thái được duy trì*] dựa trên các thuộc tính gói tin mạng sau: [chỉ định: *danh sách các thuộc tính liên kết với mỗi giao thức*].

b) loại bỏ các luồng lưu lượng hiện tại khỏi tập các luồng lưu lượng đã được thiết lập dựa trên: [lựa chọn: *thời gian chờ không hoạt động của phiên, sự hoàn tất của luồng thông tin dự kiến*].

FFW_RUL_EXT.1.6 TSF phải thực thi các quy tắc Lọc lưu lượng có trạng thái sau đây trên tất cả các lưu lượng mạng: [chỉ định: *danh sách quy tắc mặc định được áp dụng cho luồng lưu lượng mạng*].

FFW_RUL_EXT.1.7 TSF phải có khả năng loại bỏ và ghi lại theo các quy tắc sau: [chỉ định: danh sách các quy tắc cụ thể mà TOE có thể thực hiện]

FFW_RUL_EXT.1.8 TSF phải xử lý các quy tắc Lọc lưu lượng có trạng thái áp dụng theo trình tự quản trị đã xác định.

FFW_RUL_EXT.1.9 TSF phải từ chối luồng gói tin nếu quy tắc đối sánh không được xác định.

FFW_RUL_EXT.1.10 TSF phải có khả năng hạn chế số lượng [chỉ định: *các quy tắc quản lý sử dụng các tài nguyên*] đã được định cấu hình bởi quản trị.

C.3.1.2 FFW_RUL_EXT.2 Lọc trạng thái của các giao thức động

Phân cấp: Không có thành phần khác

Phụ thuộc: Không

FFW_RUL_EXT.2.1 TSF phải định nghĩa động các quy tắc hoặc thiết lập các phiên cho phép lưu lượng mạng chảy cho các giao thức mạng sau đây [chỉ định: *danh sách các giao thức được hỗ trợ*].

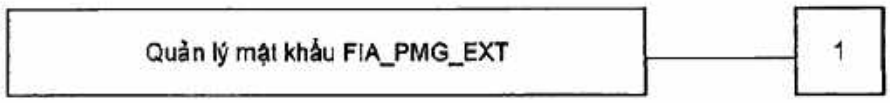
C.4 Định danh và xác thực (FIA)

C.4.1 Quản lý mật khẩu (FIA_PMG_EXT)

Tập hợp các hành vi

TOE định nghĩa các thuộc tính của mật khẩu được sử dụng bởi người dùng quản trị để đảm bảo rằng mật khẩu mạnh và cụm từ mật khẩu có thể được chọn và duy trì.

Phân cấp thành phần



FIA_PMG_EXT.1 Quản lý mật khẩu yêu cầu TSF hỗ trợ mật khẩu với các yêu cầu thành phần khác nhau, độ dài tối thiểu, tuổi thọ tối đa, và các ràng buộc tương tự.

Quản lý: FIA_PMG_EXT.1

Không có chức năng quản lý.

Kiểm toán: FIA_PMG_EXT.1

Không có yêu cầu kiểm toán cụ thể.

C.4.1.1 FIA_PMG_EXT.1 Quản lý mật khẩu

Phân cấp: Không có thành phần khác.

Phụ thuộc: Không có thành phần khác.

FIA_PMG_EXT.1.1 TSF phải cung cấp các khả năng quản lý mật khẩu sau cho các mật khẩu quản trị:

a) Mật khẩu có thể bao gồm bất kỳ sự kết hợp của chữ hoa và chữ thường, số và các ký tự đặc biệt sau đây: [chọn: "!", "@", "#", "$", "%" "^", "&", "", "(", ")", [chỉ định: các ký tự khác]];*

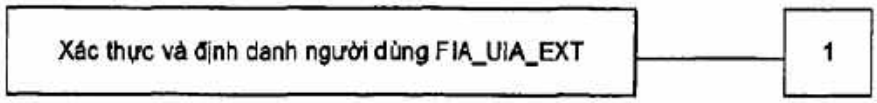
b) Chiều dài mật khẩu tối thiểu sẽ được quản trị viên an toàn thiết lập và hỗ trợ mật khẩu từ 15 ký tự trở lên.

C.4.2 Xác thực và định danh người dùng (FIA_UIA_EXT)

Tập hợp các hành vi

TSF cho phép một số hành động cụ thể trước khi thực thể không phải TOE đi qua quá trình định danh và xác thực.

Phân cấp thành phần



FIA_UIA_EXT.1 Định danh và xác thực người dùng yêu cầu quản trị viên (bao gồm cả quản trị viên từ xa) được định danh và xác thực bởi TOE, cung cấp sự đảm bảo cho đầu cuối của đường truyền thông. Nó cũng đảm bảo rằng mỗi người dùng được định danh và xác thực trước khi TOE thực hiện bất kỳ chức năng trung gian nào.

Quản lý: FIA_UIA_EXT.1

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

a) Có khả năng cấu hình danh sách các dịch vụ TOE sẵn có trước khi một thực thể được định danh và xác thực.

Kiểm toán: FIA_UIA_EXT.N

Các hành động sau cần được kiểm toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Tất cả việc sử dụng cơ chế định danh và xác thực

b) Cung cấp định người dùng, nguồn gốc của nỗ lực (ví dụ: địa chỉ IP)

C.4.2.1 FIA_UIA_EXT.1 Định danh và xác thực người dùng

Phân cấp: Không có thành phần khác.

Phụ thuộc: FTA_TAB.1 Biểu ngữ truy cập TOE mặc định

FIA_UIA_EXT.1.1 TSF phải cho phép các hành động sau đây trước khi yêu cầu các thực thể không phải là TOE bắt đầu quá trình định danh và xác thực:

- Hiển thị biểu ngữ cảnh báo theo FTA_TAB.1;
- [lựa chọn: *không có hành động khác, [chỉ định: danh sách các dịch vụ, các hành động được thực hiện bởi TSF để đáp ứng yêu cầu không phải là TOE.*]]

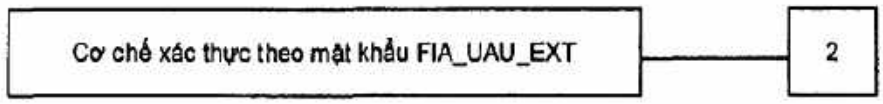
FIA_UIA_EXT.1.2 TSF phải yêu cầu mỗi người dùng quản trị phải được định danh và xác thực thành công trước khi cho phép bất kỳ hành động nào khác qua trung gian TSF thay mặt cho người dùng quản trị đó.

C.4.3 Xác thực người dùng (FIA_UAU) (FIA_UAU_EXT)

Tập hợp các hành vi

Cung cấp cơ chế xác thực người dùng dựa trên cơ sở cục bộ

Phân cấp thành phần



FIA_UAU_EXT.2 Cơ chế xác thực theo mật khẩu cung cấp cho người dùng quản trị cơ chế xác thực cục bộ.

Quản lý: FIA_UAU_EXT.2

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

a) Không

Kiểm toán: FIA_UAU_EXT.2

Các hành động sau cần được kiểm toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Tối thiểu: Tất cả việc sử dụng cơ chế xác thực

C.4.3.1 FIA_UAU_EXT.2 Cơ chế xác thực theo mật khẩu

Phân cấp: Không có thành phần khác.

Phụ thuộc: Không

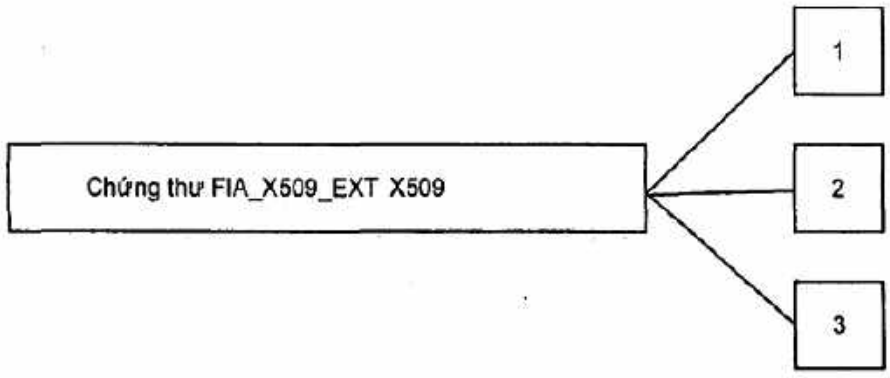
FIA_UAU_EXT.2.1 TSF phải cung cấp cơ chế xác thực dựa trên mật khẩu cục bộ, [lựa chọn: [chỉ định: cơ chế xác thực khác], không] để thực hiện chứng thực người dùng quản trị.

C.4.4 Xác thực sử dụng chứng thư X.509 (Mở rộng – FIA_X509_EXT)

Tập hợp các hành vi

Họ này định nghĩa hành vi, quản lý và sử dụng chứng thư X.509 cho các chức năng do TSF thực hiện. Các thành phần trong họ này yêu cầu xác nhận hợp lệ các chứng thư theo một bộ quy tắc cụ thể, sử dụng các chứng thư để xác thực cho các giao thức và xác minh tính toàn vẹn, và tạo ra các yêu cầu chứng thư.

Phân cấp thành phần



FIA_X509_EXT.1 Xác nhận chứng thư X.509, yêu cầu TSF kiểm tra và xác nhận hợp lệ chứng thư phù hợp với các RFC và các quy tắc được chỉ định trong thành phần.

FIA_X509_EXT.2 Xác thực chứng thư X509, yêu cầu TSF sử dụng các chứng thư để xác thực đồng nghiệp trong các giao thức hỗ trợ các chứng thư, cũng như để xác minh tính toàn vẹn và các chức năng khác cần chứng thư.

FIA_X509_EXT.3 Yêu cầu chứng thư X.509, yêu cầu TSF phải có thể tạo ra Thông điệp Yêu cầu Chứng thư và xác nhận các trả lời.

Quản lý: FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3

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

a) Xóa chứng thư X.509v3 đã nhập

b) Chấp nhận việc nhập và xóa bỏ chứng thư X.509v3

c) Khởi tạo các yêu cầu chứng thư.

Kiểm toán: FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3

Các hành động sau cần được kiểm toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Tối thiểu: Không quy định cụ thể các yêu cầu kiểm toán.

C.4.4.1 FIA_X509_EXT.1 Xác nhận chứng thư X.509

Phân cấp: Không có thành phần khác

Phụ thuộc: Không có thành phần khác

FIA_X509_EXT.1.1 TSF phải xác nhận chứng thư theo các quy tắc sau:

- Xác nhận hợp lệ chứng thư của RFC 5280 và xác nhận đường dẫn chứng thư.
- Đường dẫn chứng thư phải kết thúc với một chứng thư CA đáng tin cậy.
- TSF phải xác nhận một đường dẫn chứng thư bằng cách đảm bảo sự hiện diện của phần mở rộng cơ bản Constraints và cờ CA được đặt thành TRUE cho tất cả các chứng thư CA.
- TSF phải xác nhận tình trạng thu hồi chứng thư bằng cách sử dụng [lựa chọn: *Giao thức trạng thái chứng thư trực tuyến (OCSP) theo quy định tại RFC 2560, một danh sách thu hồi chứng thư (CRL) như được quy định trong RFC 5759*].
- TSF phải xác nhận hợp lệ trường extendedKeyUsage theo các quy tắc sau: [chỉ định: *các quy tắc chi phối nội dung của trường extendedKeyUsage cần được xác minh*].

Chú thích áp dụng: FIA_X509_EXT.1.1 liệt kê các quy tắc để xác nhận chứng thư. Tác giả ST lựa chọn xem trạng thái thu hồi có được xác minh bằng OCSP hay các CRL hay không. Tác giả ST điền vào chỉ định với các quy tắc có thể áp dụng cho các yêu cầu khác trong ST. Ví dụ: nếu một giao thức

như TLS sử dụng chứng thư được chỉ định trong ST, thì có thể chỉ định các giá trị nhất định cho trường extendedKeyUsage (ví dụ: "Máy chủ Xác thực Mục đích").

FIA_X509_EXT.1.2 TSF chỉ coi một chứng thư là một chứng thư CA nếu có phần mở rộng Hạn chế cơ bản và cờ CA được đặt thành TRUE.

Chú thích áp dụng: Yêu cầu này áp dụng cho các chứng thư được TSF sử dụng và xử lý và hạn chế các chứng thư có thể được thêm vào như là chứng thư CA đáng tin cậy.

C.4.4.2 FIA_X509_EXT.2 Xác thực chứng thư X509

Phân cấp: Không có thành phần khác

Phụ thuộc: Không có thành phần khác

FIA_X509_EXT.2.1 TSF phải sử dụng chứng thư X.509v3 theo quy định của RFC 5280 để hỗ trợ chứng thực cho [lựa chọn: *IPsec, TLS, HTTPS, SSH, [chỉ định: các giao thức khác], không có giao thức*] và [lựa chọn: *ký mã cho hệ thống cập nhật phần mềm, ký mã để xác minh tính toàn vẹn, [chỉ định: sử dụng khác], không sử dụng thêm*].

Chú thích áp dụng: Nếu TOE xác định việc thực hiện các giao thức truyền thông mà chứng thực mạng ngang hàng sử dụng các chứng thư, Tác giả ST chọn hoặc gán các giao thức đã được chỉ định; nếu không, họ chọn "không có giao thức". TOE cũng có thể sử dụng chứng thư cho các mục đích khác; lựa chọn và chỉ định thứ hai sẽ được sử dụng để xác định cụ thể những trường hợp này.

FILE_X509_EXT.2.2 Khi TSF không thể thiết lập kết nối để xác định tính hợp lệ của chứng thư, TSF phải *[lựa chọn: cho phép quản trị viên chọn chấp nhận chứng thư trong các trường hợp này, chấp nhận chứng thư, không chấp nhận chứng thư].*

Chú thích áp dụng: Thông thường một kết nối phải được thiết lập để kiểm tra tình trạng thu hồi của chứng thư - hoặc để tải xuống một CRL hoặc để thực hiện một tra cứu bằng cách sử dụng OCSP. Lựa chọn được sử dụng để mô tả hành vi trong trường hợp không thể thiết lập kết nối như vậy (ví dụ do lỗi mạng). Nếu TOE đã xác định chứng thư hợp lệ theo tất cả các quy tắc khác trong FIA_X509_EXT.1, hành vi được chỉ định trong lựa chọn sẽ xác định tính hợp lệ.

C.4.4.3 FIA_X509_EXT.3 Yêu cầu chứng thư X.509

Phân cấp: Không có thành phần khác

Phụ thuộc: Không có thành phần khác

FIA_X509_EXT.3.1 TSF phải tạo ra một Thông điệp Yêu cầu Chứng thư theo quy định của RFC 2986 và có thể cung cấp các thông tin sau trong yêu cầu: khóa công khai và [lựa chọn: *thông tin cụ thể về thiết bị, tên chung, tổ chức, đơn vị tổ chức, quốc gia, [chỉ định: các thông tin khác]*].

FIA_X509_EXT.3.2 TSF phải xác nhận chuỗi chứng thư từ CA gốc khi nhận được Phản hồi Chứng thư CA.

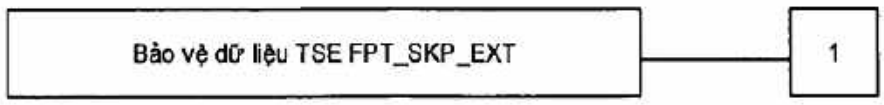
C.5 Bảo vệ TSF (FPT)

C.5.1 Bảo vệ dữ liệu TSF (FPT_SKP_EXT)

Tập hợp các hành vi

Các thành phần trong họ này đề cập các yêu cầu đối với việc quản lý và bảo vệ dữ liệu TSF, chẳng hạn như các khóa mật mã. Đây là một họ mới được mô hình sau lớp FPT_PTD.

Phân cấp thành phần



FPT_SKP_EXT.1 Bảo vệ dữ liệu TSF (để đọc tất cả các khóa đối xứng), yêu cầu người dùng hoặc chủ thể không đọc được các khóa đối xứng. Đây là thành phần duy nhất của họ này.

Quản lý: FPT_SKP_EXT.1

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

a) Không có hoạt động quản lý nào dự kiến.

Kiểm toán: FPT_SKP_EXT.1

Các hành động sau cần được kiểm toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Không có sự kiện báo cáo trước.

C.5.1.1 FPT_SKP_EXT.1 Bảo vệ dữ liệu TSF (để đọc tất cả các khóa đối xứng)

Phân cấp:	Không có thành phần khác
Phụ thuộc:	Không có thành phần khác

FPT_SKP_EXT.1.1 TSF phải ngăn không cho đọc tất cả các khóa đã chia sẻ, các khóa đối xứng và các khóa riêng.

Chú thích áp dụng: Mục đích của yêu cầu này là để thiết bị bảo vệ các khóa, tài liệu quan trọng và các ủy nhiệm xác thực khỏi việc tiết lộ trái phép. Dữ liệu này chỉ nên được truy cập cho các mục đích của chức năng an toàn được chỉ định của chúng và không cần phải hiển thị/truy cập vào bất kỳ lúc nào khác. Yêu cầu này không ngăn thiết bị cung cấp chỉ báo rằng những dữ liệu này đang tồn tại, đang được sử dụng hoặc vẫn còn hiệu lực. Tuy nhiên, nó hạn chế việc đọc ngay các giá trị này.

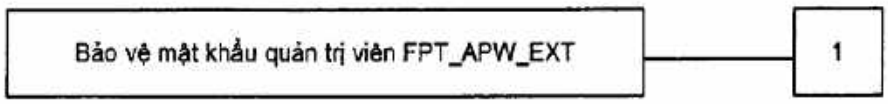
C.5.2 Bảo vệ mật khẩu quản trị viên (FPT_APW_EXT)

C.5.2.1 FPT_APW_EXT.1 Bảo vệ mật khẩu quản trị viên

Tập hợp các hành vi

Các thành phần trong họ này đảm bảo rằng TSF sẽ bảo vệ dữ liệu ủy nhiệm chứng thực bản rõ như các mật khẩu khỏi bị tiết lộ trái phép.

Phân cấp thành phần



PT_APW_EXT.1 Bảo vệ mật khẩu quản trị viên yêu cầu TSF ngăn không cho người dùng hoặc chủ thể đọc dữ liệu thông tin bản rõ thuần túy.

Quản lý: FPT_APW_EXT.1

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

a) Không có chức năng quản lý.

Kiểm toán: FPT_APW_EXT.1

Các hành động sau cần được kiểm toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Không cần kiểm toán.

Phân cấp: Không có thành phần khác

Phụ thuộc: Không có thành phần khác

FPT_APW_EXT.1.1 TSF phải lưu trữ mật khẩu ở dạng không phải là bản rõ.

FPT_APW_EXT.1.2 TSF phải ngăn chặn việc đọc các mật khẩu ở dạng bản rõ.

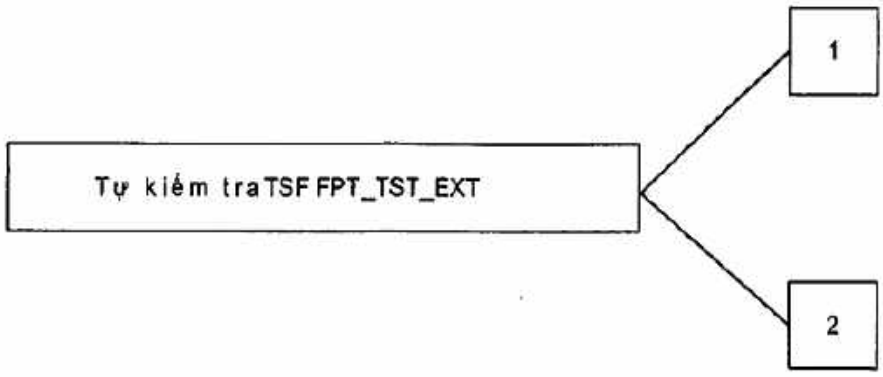
C.5.3 Tự kiểm tra TSF

C.5.3.1 FPT_TST_EXT.1 Kiểm tra TSF

Tập hợp các hành vi

Các thành phần trong họ này đưa ra các yêu cầu tự kiểm tra TSF cho hoạt động chính xác đã được lựa chọn.

Phân cấp thành phần



FPT_TST_EXT.1 Tự kiểm tra TSF đòi hỏi một bộ bài tự kiểm tra được chạy trong quá trình khởi động ban đầu để chứng minh hoạt động chính xác của TSF.

FPT_TST_EXT.2 Tự kiểm tra dựa trên chứng thư sẽ áp dụng khi sử dụng chứng thư như là một phần của tự kiểm tra, và yêu cầu tự kiểm tra không thành công nếu một chứng thư không hợp lệ.

Quản lý: FPT_TST_EXT.1, FPT_TST_EXT.2

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

a) Không có chức năng quản lý.

Kiểm toán: FPT_TST_EXT.1, FPT_TST_EXT.2

Các hành động sau cần được kiểm toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Cho biết rằng tự kiểm tra TSF đã được hoàn thành

Phân cấp: Không có thành phần khác.

Phụ thuộc: Không

FPT_TST_EXT.1.1 TSF phải chạy một loạt các bài tự kiểm tra sau [lựa chọn: *trong quá trình khởi động ban đầu (bật nguồn), định kỳ trong quá trình hoạt động bình thường, theo yêu cầu của người sử dụng được ủy quyền, tại các điều kiện [chỉ định: mà tự kiểm tra nên xảy ra]*] để chứng minh hoạt động chính xác của TSF: [chỉ định: *danh sách tự kiểm tra chạy bởi TSF*].

Chú thích áp dụng 1: Người ta hy vọng thao tác tự kiểm tra được thực hiện trong quá trình khởi động ban đầu (khi bật nguồn). Các lựa chọn khác chỉ nên được sử dụng nếu nhà phát triển có thể giải thích lý do tại sao chúng không được thực hiện trong quá trình khởi động ban đầu. Người ta hy vọng ít nhất là thao tác tự kiểm tra để xác minh tính toàn vẹn của phần sụn và phần mềm cũng như hoạt động chính xác của các chức năng mật mã cần thiết để đáp ứng các SFR sẽ được thực hiện. Nếu không phải tất cả tự kiểm tra được thực hiện trong thời gian khởi động, sẽ cần lặp lại nhiều lần của SFR này với các tùy chọn thích hợp được chọn. Trong các phiên bản tương lai của tiêu chuẩn này, bộ các bài tự kiểm tra sẽ được yêu cầu để có ít nhất các cơ chế cho khởi động được đo lường bao gồm các bài tự kiểm tra các thành phần cần thực hiện đo lường.

Chú thích áp dụng 2: Nếu các chứng thư được sử dụng bởi cơ chế tự kiểm tra (ví dụ để xác minh chữ ký để xác minh tính toàn vẹn), các chứng thư được xác thực theo FIA_X509_EXT.1 và nên được chọn trong FIA_X509_EXT.2.1. Thêm vào đó, FPT_TST_EXT.2 phải được đưa vào ST.

Phân cấp: Không có thành phần khác.

Phụ thuộc: Không

FPT_TST_EXT.2.1 TSF phải không tự kiểm tra nếu một chứng thư được sử dụng để tự kiểm tra và chứng thư tương ứng được coi là không hợp lệ.

Chú thích áp dụng: Các chứng thư có thể được sử dụng để tự kiểm tra (FPT_TST_EXT.1.1). Thành phần này phải được bao gồm trong ST nếu các chứng thư được sử dụng để tự kiểm tra. Nếu "code signing để xác minh tính toàn vẹn" được chọn trong FIA_X509_EXT.2.1, FPT_TST_EXT.2 phải được bao gồm trong ST.

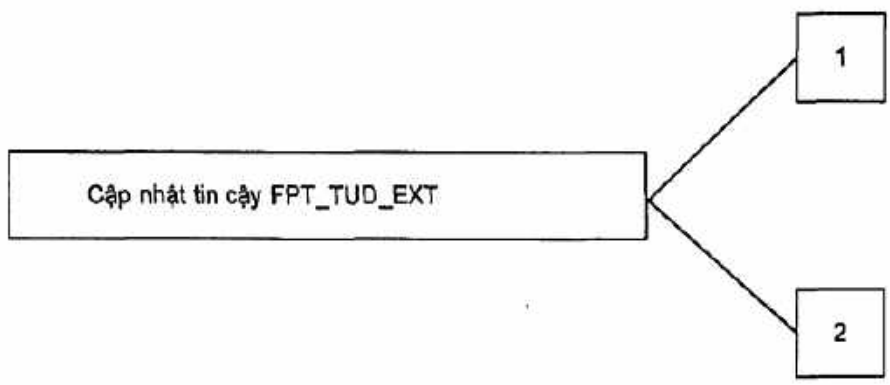
Hiệu lực được xác định bởi đường dẫn chứng thư, ngày hết hạn và trạng thái thu hồi theo FIA_X509_EXT.1.

C.5.4 Cập nhật tin cậy (FPT_TUD_EXT)

Tập hợp các hành vi

Các thành phần trong họ này đưa ra các yêu cầu để cập nhật phần sụn và/hoặc phần mềm TOE.

Phân cấp thành phần



FPT_TUD_EXT.1 Cập nhật tin cậy yêu cầu phải cung cấp các công cụ quản lý để cập nhật phần sụn và phần mềm TOE, bao gồm khả năng xác minh các bản cập nhật trước khi cài đặt.

FPT_TUD_EXT.2 Cập nhật tin cậy dựa trên chứng thư được áp dụng khi sử dụng các chứng thư như một phần của bản cập nhật tin cậy và yêu cầu cập nhật không cài đặt nếu chứng thư không hợp lệ.

Quản lý: FPT_TUD_EXT.1

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

a) Khả năng cập nhật TOE và xác minh bản cập nhật

b) Khả năng cập nhật TOE và xác minh các bản cập nhật sử dụng khả năng chữ ký số (FCS_COP.1(2)) và [lựa chọn: *không có các chức năng khác, [chỉ định: các chức năng mật mã khác hoặc các chức năng khác được sử dụng để hỗ trợ khả năng cập nhật]*]

c) Khả năng cập nhật TOE, và xác minh các bản cập nhật bằng cách sử dụng [lựa chọn: *chữ ký số, hàm băm đã công bố, không có cơ chế khác*] trước khi cài đặt những bản cập nhật này.

Kiểm toán: FPT_TUD_EXT.1

Các hành động sau cần được kiểm toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Bắt đầu quá trình cập nhật.

b) Bất kỳ lỗi nào để xác minh tính toàn vẹn của bản cập nhật.

C.5.4.1 FPT_TUD_EXT.1 Cập nhật tin cậy

Phân cấp: Không có thành phần khác

Phụ thuộc: FCS_COP.1(1) Hành động mã hóa (đối với chữ ký mã hóa) hoặc FCS_COP.1(3) Hành động mã hóa (đối với hàm băm mã hóa)

FPT_TUD_EXT.1.1 TSF phải cung cấp cho [chỉ định: *người dùng được ủy quyền*] khả năng truy vấn phiên bản hiện tại đang thực hiện của phần sụn/phần mềm TOE cũng như phiên bản phần sụn/phần mềm TOE được cài đặt gần đây nhất.

Chú thích áp dụng: Phiên bản hiện đang chạy (đang được thực thi) có thể không phải là phiên bản được cài đặt gần đây nhất. Ví dụ, có thể bản cập nhật đã được cài đặt nhưng hệ thống yêu cầu khởi động lại trước khi bản cập nhật này sẽ chạy. Do đó, cần rõ ràng là truy vấn này phải chỉ ra cả phiên bản được thực hiện gần đây nhất cũng như bản cập nhật được cài đặt gần đây nhất.

FPT_TUD_EXT.1.2 TSF phải cung cấp cho [chỉ định: *người dùng được ủy quyền*] khả năng khởi tạo cập nhật phần sụn/ phần mềm TOE theo cách thủ công và [lựa chọn: *hỗ trợ tự động kiểm tra cập nhật, hỗ trợ cập nhật tự động, không có cơ chế cập nhật khác*].

Chú thích áp dụng: Lựa chọn trong FPT_TUD_EXT.1.2 phân biệt sự hỗ trợ tự động kiểm tra cập nhật và hỗ trợ cập nhật tự động. Tùy chọn đầu tiên đề cập đến TOE để kiểm tra xem có bản cập nhật mới hay không, thông báo cho quản trị viên (ví dụ thông qua tin nhắn trong phiên quản trị, thông qua tệp nhật ký) nhưng yêu cầu một số hành động của quản trị viên để thực hiện cập nhật. Tùy chọn thứ hai đề cập đến TOE kiểm tra các bản cập nhật và tự động cài đặt chúng khi có sẵn.

FPT_TUD_EXT.1.3 TSF phải cung cấp phương tiện để xác thực bản cập nhật phần sụn/ phần mềm cho TOE sử dụng cơ chế chữ ký số, hàm băm đã được công bố) trước khi cài đặt các bản cập nhật đó.

Chú thích áp dụng 1: Cơ chế chữ ký số được tham chiếu trong lựa chọn của FPT_TUD_EXT.1.3 là một trong các thuật toán được xác định trong FCS_COP.1 (2). Hàm băm đã được công bố được tham

chiếu trong FPT_TUD_EXT.1.3 là được tạo ra bởi một trong các hàm chỉ định trong FCS_COP.1 (3). Tác giả ST nên chọn cơ chế thực hiện bởi TOE; có thể chấp nhận được nếu thực hiện cả hai cơ chế.

Chú thích áp dụng 2: Các phiên bản tương lai của tiêu chuẩn này sẽ bắt buộc sử dụng một cơ chế chữ ký số để cập nhật tin cậy.

Chú thích áp dụng 3: Nếu các chứng thư được sử dụng bởi cơ chế xác minh cập nhật, các chứng thư sẽ được xác nhận theo FIA_X509_EXT.1 và cần được chọn trong FIA_X509_EXT.2.1. Thêm vào đó, FPT_TUD_EXT.2 phải được đưa vào ST.

Chú thích áp dụng 4: "Cập nhật" trong ngữ cảnh của SFR này đề cập đến quá trình thay thế một thành phần phần mềm thường trú không ổn định, bằng một thành phần khác. Bản trước đó được gọi là hình ảnh NV, và bản sau đó là hình ảnh cập nhật. Trong khi hình ảnh cập nhật thường là mới hơn hình ảnh NV, đây không phải là một yêu cầu. Có những trường hợp hợp pháp mà chủ sở hữu hệ thống có thể muốn chuyển một thành phần sang một phiên bản cũ hơn (ví dụ khi nhà sản xuất linh kiện phát hành bản cập nhật bị lỗi hoặc khi hệ thống dựa vào tính năng không được lập tài liệu mà không còn có trong bản cập nhật). Tương tự như vậy, chủ sở hữu có thể muốn cập nhật cùng một phiên bản với hình ảnh NV để phục hồi từ bộ nhớ bị lỗi.

Tất cả các thành phần phần mềm rời rạc (ví dụ: ứng dụng, trình điều khiển, phần nhân, phần sụn) của TSF phải được nhà sản xuất tương ứng ký số và sau đó được xác minh bởi cơ chế thực hiện cập nhật. Do các thành phần này có thể được ký bởi các nhà sản xuất khác nhau, nên cần thiết quá trình cập nhật phải xác minh rằng cả bản cập nhật và hình ảnh NV đã được tạo ra bởi cùng một nhà sản xuất (ví dụ bằng cách so sánh các khóa công khai) hoặc đã được ký bởi các khóa ký hợp pháp (ví dụ xác nhận thành công các chứng thư số khi sử dụng chứng thư X.509).

C.5.4.2 FPT_TUD_EXT.2 Cập nhật tin cậy dựa trên chứng thư

Phân cấp: Không có thành phần khác

Phụ thuộc: FPT_TUD_EXT.1

FPT_TUD_EXT.2.1 TSF phải không cài đặt bản cập nhật nếu chứng thư code signing được coi là không hợp lệ.

FPT_TUD_EXT.2.2 Khi chứng thư được coi là không hợp lệ vì chứng thư này đã hết hạn, TSF phải [lựa chọn: *cho phép quản trị viên chọn chấp nhận chứng thư trong các trường hợp này, chấp nhận chứng thư, không chấp nhận chứng thư*].

Chú thích áp dụng: Các chứng thư có thể được sử dụng để ký code signing các bản cập nhật phần mềm hệ thống (FPT_TUD_EXT.1.3). Thành phần này phải được bao gồm trong ST nếu các chứng thư được sử dụng để xác nhận các bản cập nhật. Nếu "code signing cho các bản cập nhật phần mềm hệ thống" được chọn trong FIA_X509_EXT.2.1, FPT_TUD_EXT.2 phải được bao gồm trong ST.

Hiệu lực được xác định bởi đường dẫn chứng thư, ngày hết hạn và trạng thái thu hồi theo FIA_X509_EXT.1. Đối với các chứng thư đã hết hạn, tác giả của ST lựa chọn xem chứng thư số có được chấp nhận, không chấp nhận hoặc sự lựa chọn được dành cho quản trị viên để chấp nhận hoặc từ chối chứng thư.

C.6 Truy cập TOE (FTA)

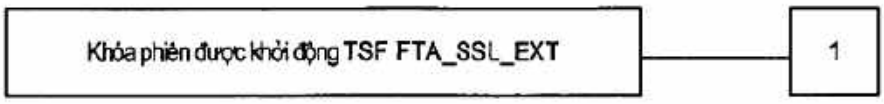
C.6.1 FTA_SSL_EXT.1 Khóa phiên được TSF khởi tạo

Tập hợp các hành vi

Các thành phần trong họ này đề cập các yêu cầu về khóa, mở khóa và chấm dứt các phiên tương tác do TSF khởi tạo và do người dùng khởi tạo.

Họ FTA_SSL_EXT mở rộng được dựa trên họ FTA_SSL.

Phân cấp thành phần



FTA_SSL_EXT.1 Khóa phiên được TSF khởi tạo, yêu cầu khóa một phiên tương tác sau một khoảng thời gian không hoạt động được khởi tạo bởi hệ thống. Đây là thành phần duy nhất của họ này.

Quản lý: FTA_SSL_EXT.1

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

a) Thông số kỹ thuật về thời gian không hoạt động của người sử dụng sau đó khóa sẽ thực hiện đối với một người dùng cá nhân.

Kiểm toán: FTA_SSL_EXT.1

Các hành động sau cần được kiểm toán nếu Tạo dữ liệu kiểm toán an toàn FAU_GEN được bao gồm trong PP/ST:

a) Bất kỳ nỗ lực nào khi mở khóa phiên tương tác.

Phân cấp: Không có thành phần khác

Phụ thuộc: FIA_UAU.1 Thời gian xác thực

FTA_SSL_EXT.1.1 TSF phải, đối với các phiên tương tác cục bộ, [lựa chọn:

- *Khóa phiên - vô hiệu hóa bất kỳ hoạt động nào của các thiết bị truy cập/hiển thị dữ liệu của người dùng khác ngoài việc mở khóa phiên, và yêu cầu quản trị viên xác thực lại cho TSF trước khi mở khóa phiên;*
- *chấm dứt phiên]*

sau một khoảng thời gian không hoạt động được xác định bởi quản trị viên an toàn.

Phụ lục D

(Quy định)

Tài liệu và đánh giá Entropy

D.0 Giới thiệu

Phụ lục này mô tả các thông tin bổ sung cần thiết cho mỗi nguồn entropy được sử dụng bởi TOE.

Tài liệu của (các) nguồn entropy phải đủ chi tiết để sau khi đọc, đánh giá viên sẽ hiểu sâu sắc nguồn entropy và tại sao có thể dựa vào nó để cung cấp đầy đủ entropy. Tài liệu này nên bao gồm nhiều phần chi tiết: mô tả thiết kế, biện minh entropy, điều kiện hoạt động và thử nghiệm mức độ chịu đựng. Tài liệu này không bắt buộc phải là một phần của TSS.

D.1 Mô tả thiết kế

Tài liệu phải bao gồm thiết kế của mỗi nguồn entropy như một tổng thể, bao gồm sự tương tác của tất cả các thành phần nguồn entropy. Bất kỳ thông tin nào có thể được chia sẻ liên quan đến thiết kế cũng nên được bao gồm cho bất kỳ các nguồn entropy bên thứ ba nào có trong sản phẩm.

Tài liệu phải mô tả hoạt động của nguồn entropy bao gồm entropy được xử lý như thế nào, và làm thế nào dữ liệu chưa xử lý (thô) có thể được lấy từ trong nguồn entropy cho các mục đích thử nghiệm. Tài liệu cần mô tả các bước thiết kế nguồn entropy cho biết entropy xuất phát từ đâu, nơi đầu ra entropy được truyền tiếp theo, bất kỳ quá trình xử lý sau đối với các đầu ra thô (hash, XOR...), có không/nơi nào nó được lưu trữ, và cuối cùng, làm thế nào để xuất ra từ nguồn entropy. Bất kỳ điều kiện nào đặt ra cho quá trình (ví dụ: chặn) cũng phải được mô tả trong thiết kế nguồn entropy. Các sơ đồ và ví dụ được khuyến khích.

Thiết kế này cũng phải bao gồm mô tả nội dung của ranh giới an ninh của nguồn entropy và mô tả cách ranh giới an ninh đảm bảo rằng kẻ địch bên ngoài ranh giới không thể ảnh hưởng đến tỷ lệ entropy.

Nếu được thực hiện, mô tả thiết kế phải bao gồm mô tả về cách các ứng dụng của bên thứ ba có thể thêm entropy vào RBG. Mô tả của bất kỳ trạng thái của RBG được lưu lại giữa lúc tắt nguồn và bật nguồn phải được đưa vào.

D.2 Biện minh Entropy

Cần phải có một luận cứ kỹ thuật về tính không thể dự đoán trước được trong nguồn đến từ đâu và tại sao lại đặt tin tưởng là nguồn entropy cung cấp đầy đủ entropy cho các sử dụng đầu ra RBG (bởi TOE cụ thể này). Luận cứ này sẽ bao gồm một mô tả về tỉ lệ entropy tối thiểu mong muốn (tức là entropy tối thiểu (theo bit) cho mỗi bit hoặc byte của dữ liệu nguồn) và giải thích rằng entropy đầy đủ đang đi vào quá trình tạo hạt ngẫu nhiên TOE. Thảo luận này sẽ là một phần của việc giải thích lý do tại sao có thể dựa vào nguồn entropy để tạo ra các bit có entropy.

Số lượng thông tin cần thiết để biện minh cho tỷ lệ entropy tối thiểu mong muốn tùy thuộc vào loại nguồn entropy bao gồm trong sản phẩm.

Đối với các nguồn entropy do nhà phát triển cung cấp, để xác định tỷ lệ entropy tối thiểu, người ta mong muốn một số lượng lớn các bit nguồn thô sẽ được thu thập, các phép thử thống kê sẽ được thực hiện, và tỷ lệ entropy tối thiểu được xác định từ các phép thử thống kê. Mặc dù không có các phép thử thống kê nào được yêu cầu tại thời điểm này, người ta hy vọng rằng một số phép thử là cần thiết để xác định lượng entropy tối thiểu ở mỗi đầu ra.

Đối với các nguồn entropy được cung cấp bởi bên thứ ba, trong đó nhà cung cấp TOE có quyền truy cập hạn chế đối với thiết kế và dữ liệu entropy thô, nguồn tài liệu sẽ chỉ ra ước tính số lượng entropy tối thiểu thu được từ nguồn của bên thứ ba này. Có thể chấp nhận nhà cung cấp "giả định" một số lượng entropy tối thiểu, tuy nhiên, giả định này phải được nêu rõ trong tài liệu cung cấp. Cụ thể, ước tính entropy tối thiểu phải được xác định và giả định phải được bao gồm trong ST.

Bất kể loại nguồn entropy như thế nào, biện minh cũng sẽ bao gồm cách DRBG được khởi tạo với entropy được nêu trong ST, ví dụ bằng cách xác minh rằng tỷ lệ entropy tối thiểu được nhân với số lượng dữ liệu nguồn được sử dụng để gieo hạt DRBG hoặc rằng tỷ lệ entropy dự kiến dựa trên số lượng dữ liệu nguồn đã được nêu rõ ràng và so sánh với tỷ lệ thống kê. Nếu số lượng dữ liệu nguồn được sử dụng để gieo hạt DRBG không rõ ràng hoặc tỷ lệ tính toán không rõ ràng liên quan đến hạt, tài liệu sẽ không được coi là hoàn chỉnh.

Biện minh entropy phải không bao gồm bất kỳ dữ liệu nào được thêm vào từ bất kỳ ứng dụng của bên thứ ba hoặc từ bất kỳ trạng thái nào lưu giữa các lần khởi động lại.

D.3 Điều kiện hoạt động

Tỷ lệ entropy có thể bị ảnh hưởng bởi các điều kiện nằm ngoài sự kiểm soát của nguồn entropy. Ví dụ, điện áp, tần số, nhiệt độ, và thời gian trôi qua sau khi bật nguồn chỉ là một vài trong số các yếu tố có thể ảnh hưởng đến hoạt động của nguồn entropy. Do đó, tài liệu cũng sẽ bao gồm nhiều điều kiện hoạt động mà ở đó nguồn entropy được mong đợi sẽ tạo ra dữ liệu ngẫu nhiên. Tương tự, tài liệu sẽ mô tả các điều kiện mà ở đó nguồn entropy không còn đảm bảo cung cấp đủ entropy. Các phương pháp sử dụng để phát hiện hư hỏng hoặc suy thoái của nguồn phải được đưa vào.

D.4 Thử nghiệm mức độ chịu đựng

Cụ thể hơn, tất cả các thử nghiệm mức độ chịu đựng nguồn entropy và lý do của chúng sẽ được ghi lại. Điều này bao gồm mô tả các bài thử nghiệm mức độ chịu đựng, tỷ lệ và các điều kiện ở đó mỗi thử nghiệm mức độ chịu đựng được thực hiện (ví dụ, khi khởi động, khi hoạt động liên tục hoặc theo yêu cầu), kết quả dự kiến cho mỗi thử nghiệm mức độ chịu đựng, hành vi TOE khi nguồn entropy hư hỏng, và lý do cho thấy tại sao mỗi thử nghiệm được cho là thích hợp để phát hiện một hoặc nhiều hư hỏng trong nguồn entropy.

Thư mục tài liệu tham khảo

[1] Collaborative Protection Profile for Stateful Traffic Filter Firewalls Version 1.0 (Hồ sơ bảo vệ cho thiết bị tường lửa lọc lưu lượng có trạng thái) của CCRA, Phiên bản 1.0.