TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 12820:2020

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – HỒ SƠ BẢO VỆ CHO CHỨC NĂNG PHÒNG CHỐNG XÂM NHẬP TRÊN THIẾT BỊ TƯỜNG LỬA/THIẾT BỊ MẠNG

Information technology - Security techniques - Protection profile for intrusion prevention systems in firewalls/network devices

HÀ NỘI - 2020

Mục lục

Lời nói đầu

TCVN 12820:2020 được xây dựng dựa trên cơ sở tham khảo "collaborative Protection Profile for Network Devices/ collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS)" của Hiệp hội đảm bảo thông tin quốc gia của Hoa Kỳ NIAP, phiên bản 2.11, ngày 15/6/2017.

TCVN 12820:2020 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 chức năng phòng chống xâm nhập trên thiết bị tường lửa/ thiết bị mạng

Information Technology - Security techniques - Protection profile for Intrusion Prevention Systems in Firewalls/ Network Devices

1 Phạm vi áp dụng

Tiêu chuẩn này quy định hồ sơ bảo vệ cho chức năng phòng chống xâm nhập (chức năng IPS) trên thiết bị tường lửa/thiết bị mạng, thể hiện các yêu cầu chức năng an toàn (SFR) và yêu cầu đảm bảo an toàn (SAR) đối với chức năng phòng chống xâm nhập, phù hợp với bộ tiêu chuẩn quốc gia 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).

Các yêu cầu này là phần mở rộng của các yêu cầu đưa ra trong hồ sơ bảo vệ cho thiết bị mạng (NDPP) và hồ sơ bảo vệ cho thiết bị tường lửa (FWPP). Điều này có nghĩa một sản phẩm IPS phải đáp ứng yêu cầu an toàn của thiết bị mạng, thiết bị tường lửa và các yêu cầu phần mở rộng cho chức năng IPS trong tiêu chuẩn này.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây là cần thiết để áp dụng 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".

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

Bất thường/dị thường (anomaly/anomalous)

Hoạt động truy cập có sự khác biệt so với hoạt động bình thường của hệ thống. Hoạt động này không nhất thiết là các hoạt động xâm nhập nhưng cũng có thể xác định các hoạt động xâm nhập thông qua các hoạt động dị thường.

3.2

Thông số/hoạt động bình thường (baseline/base-lining)

Là các thông số chỉ trạng thái hoạt động bình thường của hệ thống và không có hoạt động xâm nhập.

3.3

Chế độ nội tuyến (inline mode)

Chế độ hoạt động của IPS mà cho phép lưu lượng mạng đi qua thiết bị này và được kiểm tra trước khi gửi đến hệ thống được bảo vệ. Chế độ hoạt động này cho phép IPS có thể ngăn chặn các hoạt động xâm nhập.

3.4

Hệ thống ngăn chặn xâm nhập (Intrusion Prevention System)

Các thiết bị được sử dụng để giám sát, phân tích kết nối mạng nhằm phát hiện cảnh báo và ngăn chặn tấn công mạng theo thời gian thực.

3.5

Chính sách IPS (IPS policy)

Tập hợp các luật/dấu hiệu và chính sách của IPS để thực hiện chức năng phát hiện và ngăn chặn xâm nhập.

3.6

Chuẩn hóa (của lưu lượng mạng) (normalization (of network traffic))

Hành động chuẩn hóa các gói tin trước khi gửi về hệ thống được bảo vệ khi IPS hoạt động ở chế độ nội tuyến.

3.7

Chế độ ngẫu nhiên (promiscuous mode)

Chế độ hoạt động của IPS mà cho phép IPS theo dõi thụ động hoạt động của hệ thống. Hoạt động ở chế độ này, IPS không thể thực hiện chức năng ngăn chặn xâm nhập như chế độ nội tuyến.

3.8

Giao diện cảm biến (sensor interface)

Giao diện của IPS được sử dụng để thu thập lưu lượng mạng phục vụ việc phân tích và xử lý của IPS.

4 Ký hiệu và chữ viết tắt

CC	Tiêu chí chung	Common Criteria
CCRA	Thỏa thuận công nhận tiêu chí chung	Common Criteria Recognition Arrangement
CNTT	Công nghệ thông tin	
DNS	Hệ thống tên miền	Domain Name System
FWPP	Hồ sơ bảo vệ cho thiết bị tường lửa lọc lưu lượng có trạng thái	Protection Profile for Stateful Traffic Filter Firewalls
NDPP	Hồ sơ bảo vệ cho thiết bị mạng	Protection Profile for Network Devices
EAL	Cấp đảm bảo đánh giá	Evaluation Assurance Level
ICMP	Giao thức bản tin điều khiển Internet	Internet Control Message Protocol
IDS	Thiết bị phát hiện xâm nhập	Intrusion Detection System
IDSPP	Hồ sơ bảo vệ cho thiết bị phát hiện xâm nhập	Intrusion Detection System Protection Profile
IPS	Thiết bị phòng chống xâm nhập	Intrusion Prevention System
ISMS	Hệ thống quản lý an toàn thông tin	Information Security Management System
NPU	Bộ xử lý mạng	Network Processing Unit
OSP	Chính sách an toàn tổ chức	Organizational Security Policy
PP	Hồ sơ bảo vệ	Protection Profile
SAR	Yêu cầu đảm bảo an toàn	Security Assurance Requirement
SFR	Yêu cầu chức năng an toàn	Security Functional Requirement
ST	Đích an toàn	Security Target
TOE	Đích đánh giá	Target of Evaluation
TSF	Các chức năng an toàn của TOE	TOE Security Functions
TSS	Đặc tả tóm tắt TOE	TOE summary specification
AGD	Tài liệu hướng dẫn	Guidance documents

5 Giới thiệu Hồ sơ bảo vệ

5.1 Phạm vi TOE

Hồ sơ bảo vệ cho các thiết bị mạng (NDPP) đưa ra các yêu cầu chức năng an toàn (SFR) và yêu cầu đảm bảo an toàn (SAR) cơ bản cho thiết bị mạng nói chung. Hồ sơ bảo vệ cho thiết bị tường lửa (FWPP) đưa ra các SFR và SAR tương tự như NDPP nhưng bổ sung các yêu cầu cụ thể đối với chức

năng lọc gói tin. Hồ sơ bảo vệ cho chức năng IPS trong tiêu chuẩn này kế thừa các yêu cầu trong hồ sơ bảo vệ của NDPP hoặc FWPP và bổ sung các SFR cụ thể đối với chức năng IPS.

Tiêu chuẩn này phù hợp với bộ tiêu chuẩn quốc gia 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).

5.2 Sử dụng Hồ sơ bảo vệ cho chức năng IPS trên thiết bị tích hợp

Được sử dụng như một phần mở rộng của NDPP hoặc FWPP, hồ sơ bảo vệ này sẽ được sử dụng phù hợp với việc đánh giá đích an toàn ST cụ thể tương ứng với phiên bản áp dụng của NDPP hoặc FWPP.

Khi hồ sơ bảo vệ cho chức năng IPS được xây dựng từ hồ sơ bảo vệ PP của NDPP, thì các đích đánh giá TOE phải tuân thủ các yêu cầu chức năng trong NDPP cùng với phần bổ sung cho chức năng IPS được đưa ra trong tiêu chuẩn này. Tương tự như vậy, khi hồ sơ bảo vệ này được xây dựng dựa trên PP của FWPP thì các TOE phải đáp ứng tất cả các yêu cầu của PP đó cũng như những yêu cầu mở rộng trong tiêu chuẩn này. PP của NDPP hoặc FWPP được gọi là PP cơ sở.

Việc đánh giá theo ST cho chức năng IPS cũng phải lựa chọn phù hợp với đích đánh giá của FWPP hoặc NDPP tương ứng. Trong một số trường hợp, các yêu cầu đối với chức năng IPS có thể không tương thích với yêu cầu FWPP (Ví dụ: đối với yêu cầu chức năng tường lửa FWPP sẽ cấm tất cả các gói tin theo từng dịch vụ trong khi IPS có thể cấm các gói tin theo nội dung cụ thể đối với từng dịch vụ). Tuy nhiên, trong quá trình đánh giá theo ST chức năng IPS có thể thiết lập cấu hình phù hợp để đáp ứng các yêu cầu an toàn của FWPP.

6 Phạm vi TOE

Tiêu chuẩn này đưa ra hồ sơ bảo vệ cho thiết bị phòng chống xâm nhập IPS trên môi trường mạng. tập trung vào các chức năng giám sát, phân tích kết nối mạng sử dụng giao thức IP (TCP, UDP, ICMP...). Việc tập trung vào giao thức mạng IP trong Hồ sơ này để xác định phạm vi đánh giá cũng như các yêu cầu an toàn phù hợp. Điều này cho phép các hồ sơ bảo vệ mở rộng tiếp theo có thể được xây dựng để mở rộng phạm vi đánh giá đối với các chức năng khác của chức năng IPS. Phạm vi đánh giá trong tiêu chuẩn này không bao gồm các giao thức không phải là giao thức IP (non-IP), bao gồm cả các giao thức ở lớp 2 như Ethernet.

Các yêu cầu cơ bản cho chức năng IPS trong Hồ sơ này phải có khả năng thu thập, phân tích thời gian thực kết nối mạng, bao gồm:

- Giám sát thụ động kết nối mạng trên một hoặc nhiều giao diện của IPS và/hoặc giám sát kết nối mạng đi qua TOE sử dụng chế độ nội tuyến.

Truyền dữ liệu IPS đến máy chủ lưu trữ kiểm toán bên ngoài và tùy chọn lưu trữ dữ liệu IPS bên trong. Dữ liệu kiểm toán IPS có thể được đẩy đi từ TOE hoặc tải về từ một máy khách. Bất kể cơ chế gửi dữ liệu IPS như thế nào thì dữ liệu trao đổi phải được bảo vệ theo yêu cầu FAU_STG_EXT.1 của NDPP và FWPP.

- Phân tích lưu lượng mạng dựa trên các quy tắc mà quản trị viên có thể định cấu hình trực tiếp trên TOE và tùy chọn phân tích lưu lượng mạng dựa trên các quy tắc được nhập/áp dụng từ hệ thống khác.

- Có khả năng xử lý thời gian thực, độc lập đối với các nguy cơ tấn công mạng (chặn kết nối, hủy kết nối) và có tùy chọn để xử lý với các giao thức mạng non-IP.

Có nhiều chức năng tương đương giữa thiết bị phòng chống xâm nhập IPS và thiết bị phát hiện xâm nhập IDS. Nhưng có điểm khác biệt quan trọng là IPS có chức năng ngăn chặn tấn công mạng khi phát hiện, trong khi IDS chỉ có chức năng phát hiện và cảnh báo tấn công mạng. Tuy nhiên, quản trị viên có thể thiết lập cấu hình của IPS để nó có thể hoạt động như thiết bị IDS trong quá trình thực hiện đánh giá.

Các TOE khác nhau có thể sử dụng phương pháp khác nhau để phát hiện xâm nhập dựa vào việc phân tích kết nối mạng và các dấu hiệu tấn công đã biết hoặc dựa theo hành vi dị thường để phát hiện các dạng tấn công chưa biết. Việc phát hiện tấn công mạng có thể kết hợp giữa nhiều phương pháp và dấu hiệu khác nhau.

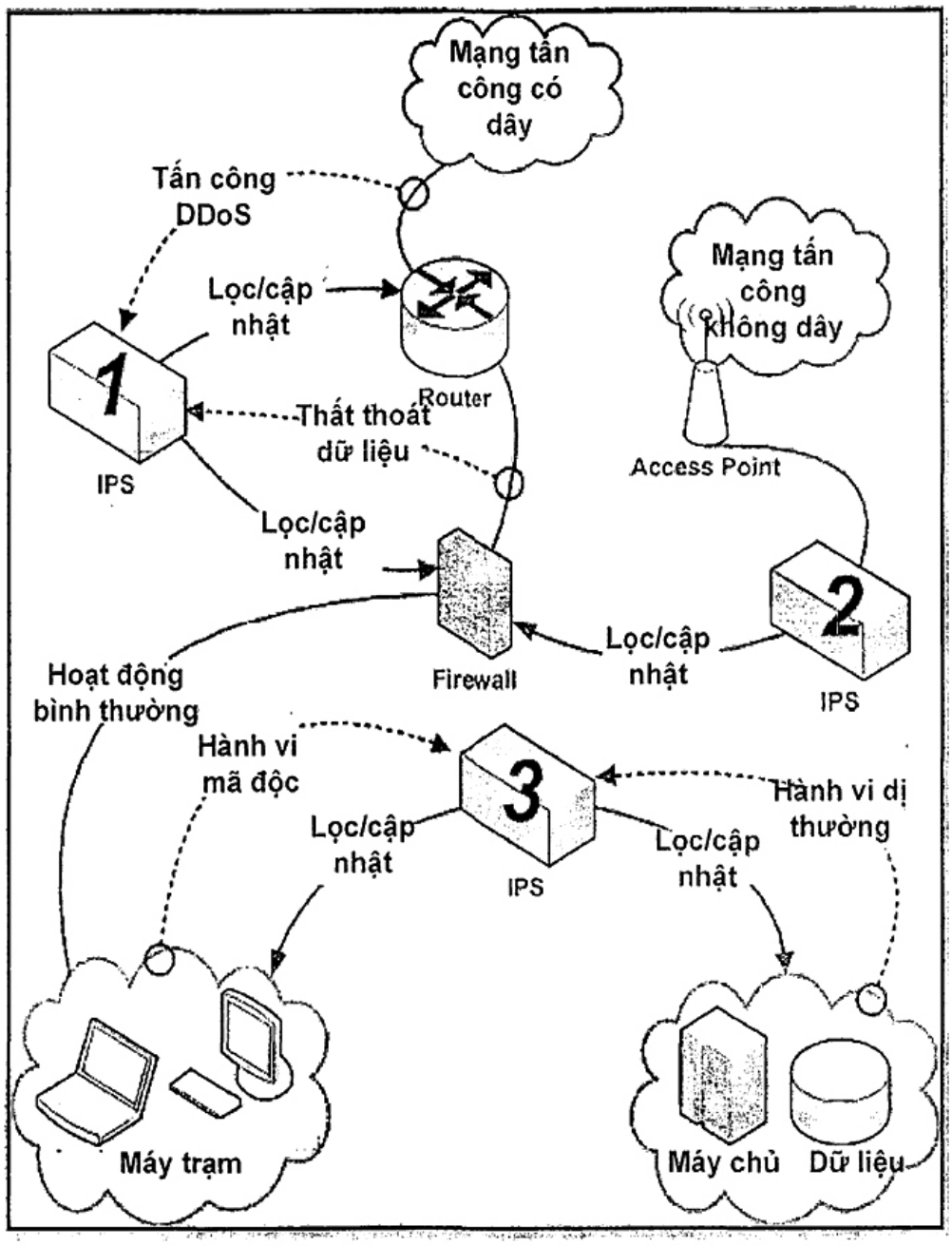
Các yêu cầu an toàn SFR của IPS sẽ khác nhau khi triển khai phân tán ở vị trí khác nhau trong mạng. Trường hợp IPS triển khai ở vị trí mạng biên thì chức năng an toàn phải thỏa mãn toàn bộ các yêu cầu han toàn của NDPP hoặc FWPP. Thêm nữa, mọi giao tiếp giữa các điểm triển khai phân tán phải được bảo vệ sử dụng giao thức mạng tin cậy theo yêu cầu trong hồ sơ bảo vệ của NDPP hoặc FWPP.

• **IPS 1** hoạt động ở chế độ promiscuous, thu thập dữ liệu mạng ở vùng mạng phía ngoài tường lửa. Trong trường hợp này, IPS hoạt động như IDS và có thể gửi các lệnh tới router biên để thực hiện ngăn chặn nguồn tấn công.

• **IPS 2** hoạt động trong chế độ nội tuyến ở lớp 2 cho phép phân tích lưu lượng mạng từ vùng mạng không dây đến các vùng mạng khác trong hệ thống. Trường hợp này, IPS có thể tự ngăn chặn các tấn công mạng theo chính sách đặt trước trên IPS và không cần tương tác với các thiết bị khác.

• **IPS 3** hoạt động kết hợp của chế độ promiscuous và chế độ nội tuyến. Trong trường hợp này IPS có chức năng định tuyến và phân tích lưu lượng mạng giữa các mạng kết nối trực tiếp với IPS.

Hình 1 dưới đây minh họa các vị trí có thể triển khai IPS trong một mạng:



Hình 1 - Sơ đồ kịch bản triển khai đích đánh giá

7 Mô tả các vấn đề an toàn

Các TOE thiết lập các tập các chính sách/luật khác nhau để phát hiện và ngăn chặn tấn công mạng trong một hệ thống mạng được bảo vệ. Các nguy cơ tấn công mạng có thể đến từ một hoặc nhiều các thiết bị đầu cuối trong mạng hoặc từ hạ tầng mạng hoặc thậm chí từ bản thân thiết bị IPS. Từ khóa "mạng được giám sát" được sử dụng ở đây để nói đến bất kỳ vùng mạng nào trong hệ thống có kết nối trực tiếp đến IPS hoặc các vùng mạng khác có lưu lượng đi qua IPS.

Thuật ngữ "Dữ liệu IPS" sẽ được sử dụng trong tiêu chuẩn này bao gồm các dữ liệu thu thập trên môi trường mạng; dữ liệu lưu trữ trên IPS; kết quả phân tích và cảnh báo, sự tương tác đối với kết của phân

tích của IPS. Dữ liệu này là khác với "dữ liệu kiểm toán" được định nghĩa trong FAU_GEN của hồ sơ bảo vệ cơ sở, giống như các dữ liệu liên quan đến xác thực và thiết lập kênh kết nối tin cậy khi quản trị IPS.

Người quản trị có thể thiết lập chính sách/luật phù hợp trên IPS để phòng chống các nguy cơ tấn công mạng đối với hệ thống của họ. Các nguy cơ tấn công mạng mà IPS có thể phòng chống như:

- Tấn công dò quét như thăm dò để thu thập thông tin trên môi trường mạng hoặc các thiết bị đầu cuối sử dụng các công nghệ dò quét và ánh xạ.

- Tấn công làm mất tính khả dụng của hạ tầng mạng, thiết bị đầu cuối, hoặc các dịch vụ, chẳng hạn như tấn công DoS/DDoS.

- Truy cập trái phép hệ thống, thiết bị đầu cuối hoặc dịch vụ thông qua các cơ chế tấn công dò quét mật khẩu, khai thác điểm yếu an toàn thông tin và đưa các mã thực thi lên thiết bị.

- Tiết lộ/lấy cắp thông tin nhạy cảm như số tài khoản, thông tin cá nhân... Chú ý là dạng dữ liệu này có thể bị lấy cắp bằng cách truy cập từ bên ngoài hoặc được gửi đi từ bên trong mạng thông qua các hình thức tấn công từ bên ngoài hay bên trong mạng.

Lưu ý rằng các mối đe dọa được xác định trong tiêu chuẩn này không lặp lại trong NDPP và FWPP mà kế thừa từ NDPP và FWPP. Ngoài ra, trong tiêu chuẩn này còn mô tả chức năng bảo mật của IPS mà các chức năng này có thể tồn tại các mối đe dọa như NDPP và FWPP. Bảng tổng hợp các mối đe dọa đối với IPS được tổng hợp trong Phụ lục A của tiêu chuẩn này.

NDPP chỉ chứa các mối đe dọa ứng với các chức năng riêng của nó. Trong khi FWPP bao gồm tất cả các mối đe dọa tương tự như NDPP nhưng thêm các mối đe dọa liên đến môi trường hoạt động của nó. Tiêu chuẩn này cũng tập trung vào các mối đe dọa liên quan đến môi trường hoạt động như FWPP nhưng có sự phù hợp với đặc trưng của chức năng IPS thay vì chỉ chức năng lọc gói như tường lửa.

7.1 Tiết lộ trái phép thông tin

Thông tin nhạy cảm không được mã hóa, khi truyền đưa trên mạng bị lộ lọt là hình thức vi phạm chính sách bảo mật của hệ thống được bảo vệ. IPS có chức năng kiểm tra nội dung các gói tin để phát hiện và xử lý các thông tin nhạy cảm phát hiện được.

(T.NETWORK_DISCLOSURE)

7.2 Truy cập trái phép

Kẻ tấn công truy cập trái phép hệ thống, thiết bị đầu cuối hoặc dịch vụ thông qua các cơ chế tấn công dò quét mật khẩu, khai thác điểm yếu an toàn thông tin và đưa các mã thực thi lên thiết bị.

(T.NETWORK_ACCESS)

7.3 Vi phạm chính sách truy cập dịch vụ

Việc tin tặc thực hiện các hình thức tấn công vào các dịch vụ được cung cấp bởi hệ thống từ các mạng bên ngoài. Thông qua các dịch vụ công cộng này tin tặc có thể thực hiện các hình thức tấn công mạng như: chèn câu truy vấn độc hại SQL, lừa đảo, buộc hủy kết nối, mã độc trong tệp tin nén, tệp tin ngụy trang, chiếm quyền điều khiển, và mạng botnet.

(T.NETWORK_MISUSE)

7.4 Tấn công từ chối dịch vụ

Tấn công vào những dịch vụ/hệ thống được cung cấp bởi hệ thống, gây nên việc các dịch vụ bị cạn kiệt tài nguyên, quá tải và làm gián đoạn hoạt động của dịch vụ/hệ thống. Mặc dù hầu hết các IPS sẽ cung cấp chức năng bảo vệ tấn công từ chối dịch vụ phân tán DDoS, nhưng chức năng này không phải là bắt buộc đối với IPS. Tuy nhiên chức năng phòng chống tấn công DoS là bắt buộc.

(T.NETWORK_DOS)

8 Các mục tiêu an toàn

Các vấn đề an toàn được mô tả trong điều 7 sẽ được xử lý bằng cách kết hợp các chức năng an toàn của IPS và vị trí triển khai IPS phù hợp trong hệ thống mạng được bảo vệ. Các mục tiêu đánh giá sẽ đưa ra các chức năng an toàn để xử lý các nguy cơ tấn công mạng mà IPS phải đáp ứng thông qua việc thu thập và giám sát lưu lượng mạng và thực thi các chính sách do người quản trị IPS thiết lập. Dưới đây là mô tả các mục tiêu an toàn cần thiết để xử lý các mối đe dọa/ chính sách ở điều 7.

CHÚ THÍCH: Trong mỗi phần dưới đây các mục tiêu an toàn cụ thể được xác định và chúng được kết hợp với các yêu cầu chức năng an toàn liên quan để đáp ứng các mục tiêu.

8.1 Giám sát hệ thống

Để có chức năng phát hiện và xử lý tấn công mạng, IPS phải có chức năng thu thập và phân tích lưu lượng mạng từ hệ thống được bảo vệ.

(O.SYSTEM_MONITORING -> FAU_ARP.1 (mục tiêu), FAU_GEN.1 / IPS, FAU_SAR.1 (mục tiêu), FAU_SAR.2 (mục tiêu), FAU_SAR.3 (mục tiêu), FAU_STG.1 (tùy chọn), FAU_STG.4 (tùy chọn), FRU_RSA (tùy chọn)).

8.2 Phân tích và phát hiện vi phạm chính sách

Các thiết bị bên trong hệ thống mạng và có giao tiếp qua môi trường mạng thường tiềm ẩn nhiều nguy cơ hoặc vi phạm chính sách của hệ thống. IPS phải có khả năng phân tích lưu lượng mạng để phát hiện các nguy cơ tấn công mạng hoặc lộ lọt thông tin.

(O.IPS_ANALYZE -> IPS_ABD_EXT.1, IPS_IPB_EXT.1, IPS_NTA_EXT.1, IPS_SBD_EXT.1, IPS_SBD_EXT.2 (tùy chọn)).

8.3 Xử lý hành vi vi phạm chính sách

IPS phải có chức năng xử lý các hành vi vi phạm chính sách phát hiện được tới người quản trị hệ thống theo các chính sách/ luật được thiết lập trước.

(O.IPS_REACT -> FAU_ARP.1 (mục tiêu), IPS_ABD_EXT.1).

8.4 Quản trị TOE

IPS phải cung cấp chức năng cho phép người quản trị có thể quản trị IPS để quản lý, giám sát hoạt động và thiết lập các chính sách/ luật cho IPS.

(O.TOE_ADMINISTRATION-> FMT_MOF.1 / IPS (tùy chọn), FMT_MTD.1 / IPS (tùy chọn), FMT_SMF.1 / IPS, FMT_SMR.2 / IPS (tùy chọn)).

8.5 Truyền thông tin cậy

IPS phải cung cấp kênh kết nối tin cậy để cho phép IPS có thể giao tiếp với các thành phần khác trong hệ thống an toàn.

(O.TRUSTED_COMMUNICATIONS (tùy chọn) -> FPT_ITT.1 (tùy chọn)).

9 Các yêu cầu an toàn

Phần này đưa ra các yêu cầu về chức năng an toàn cho IPS, cũng như xác định các hoạt động cần bảo đảm của người thực hiện đánh giá.

9.1 Quy ước

Tiêu chuẩn này định nghĩa các thao tác với các yêu cầu an toàn tương ứng của IPS bao gồm: chỉ định, lựa chọn hoặc chỉ định trong các lựa chọn và tinh chỉnh. Tiêu chuẩn này sử dụng các quy ước về phông chữ theo tiêu chuẩn chung CC:

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

• Tinh chỉnh: được trình bày đằng sau từ "**Tinh chỉnh**" và được bôi đậm;

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

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

• Lặp lại: Chỉ định bằng cách thêm các SFR hoặc thành phần tên với một dấu gạch chéo và chỉ báo duy nhất, ví dụ "/IPS".

9.2 Yêu cầu chức năng an toàn cho IPS

Là mở rộng của NDPP hoặc FWPP, tiêu chuẩn này định nghĩa một số SFR liên quan đến chức năng IPS cũng như chức năng kiểm toán và quản lý có liên quan. Yêu cầu các chức năng an toàn được đưa ra trong bảng dưới đây:

Bảng 1 - Các yêu cầu chức năng an toàn

Tên lớp	Xác định thành phần	Tên thành phần
FAU: Kiểm toán an toàn	FAU_GEN.1/IPS	Tạo dữ liệu kiểm toán an toàn (IPS)
FMT: Quản lý an toàn	FMT_SMF.1/IPS	Chức năng quản trị (IPS)
IPS: Ngăn chặn xâm nhập	IPS_ABD_EXT.1	Chức năng IPS phát hiện hoạt động dị thường
	IPS_IPB_EXT.1	Chức năng khóa địa chỉ IP
	IPS_NTA_EXT.1	Chức năng phân tích lưu lượng mạng
	IPS_SBD_EXT.1	Chức năng IPS phát hiện tấn công theo dấu hiệu (signature)

9.2.1 FAU: Kiểm toán an toàn

9.2.1.1 FAU_GEN.1/IPS: Tạo dữ liệu kiểm toán an toàn (IPS)

FAU_GEN.1.1/IPS Tinh chỉnh: TSF có thể tạo ra bản ghi kiểm toán **IPS** trong các sự kiện IPS có thể kiểm toán **IPS** sau:

a) Khởi động và tắt các chức năng **IPS;**

b) Tất cả các sự kiện có thể kiểm toán **IPS** cho [chưa được chi tiết] mức độ kiểm toán; và

~~*c) Tất cả các hành động quản trị;*~~

d) [Tất cả các sự kiện khác nhau của IPS;

e) Tất cả các phản ứng khác nhau của IPS;

e) Tổng số các sự kiện tương tự xảy ra trong một khoảng thời gian xác định; và

g) Tổng số các phản ứng tương tự xảy ra trong một khoảng thời gian xác định.]

FAU_GEN.1.2/IPS Tinh chỉnh: TSF sẽ lưu lại trong mỗi bản ghi **sự kiện có thể kiểm toán IPS** bao gồm ít nhất các thông tin sau:

a) Ngày và thời gian của sự kiện, loại sự kiện **và/hoặc phản ứng**, ~~định danh chủ thể, và kết quả (thành công hay thất bại) của sự kiện~~;

b) Đối với mỗi loại sự kiện **có thể kiểm toán IPS**, dựa trên định nghĩa về sự kiện có thể kiểm toán của các thành phần chức năng trong PP/~~ST~~, [*các sự kiện có thể kiểm toán xác định cụ thể trong Bảng 2*].

Bảng 2 – Các sự kiện có thể kiểm toán và nội dung bản ghi kiểm toán bổ sung

Yêu cầu	Các sự kiện có thể kiểm toán	Nội dung bản ghi kiểm toán bổ sung
FMT_SMF.1/IPS	Chỉnh sửa một phần tử chính	Định danh hoặc tên của phần tử

	sách IPS	chính sách IPS bị chỉnh sửa (ví dụ, dấu hiệu, đường cơ sở, danh sách sạch hoặc danh sách đen).
IPS_ABD_EXT.1	Phát hiện các gói tin khớp với dấu hiệu dị thường theo chính sách IPS	Địa chỉ IP nguồn-đích
		Nội dung các trường mào đầu của gói tin.
		Giao diện TOE nhận được gói tin.
		Các chính sách phát hiện dấu hiệu dị thường (ví dụ thông lượng, thời gian trong ngày, tần suất sự kiện...).
		Các hành động xử lý bởi TOE khi gói tin khớp luật của IPS (ví dụ: cho phép, chặn, gửi lệnh thiết lập lại tới IP nguồn, gửi lệnh thông báo chặn đến Firewall...).
IPS_IPB_EXT.1	Phát hiện gói tin có địa chỉ IP nằm trong danh sách sạch hoặc danh sách đen.	Các địa chỉ IP nguồn và đích (chỉ báo địa chỉ nguồn và/hoặc địa chỉ đích nằm trong danh sách sạch hoặc danh sách đen, nếu áp dụng).
		Giao diện TOE nhận được gói tin.
		Các hành động xử lý của TOE khi gói tin khớp luật (ví dụ: cho phép, chặn, gửi lệnh thiết lập lại...).
IPS_NTA_EXT.1	Thay đổi chính sách IPS áp dụng trên giao diện của IPS Cho phép/cấm giao diện của TOE với chính sách IPS áp dụng. Thay đổi các chế độ thiết lập trên giao diện của IPS.	Định danh giao diện của TOE.
		Chính sách IPS và chế độ hoạt động của giao diện (nếu áp dụng).
IPS_SBD_EXT.1	Kiểm tra các gói tin khớp luật dựa trên dấu hiệu (signature) của IPS với chức năng ghi log	Tên hoặc định danh của dấu hiệu đã khớp.
		Địa chỉ IP nguồn và đích.

	được mở.	Nội dung của các trường mào đầu được xác định khớp với dấu hiệu.
		Giao diện TOE đã nhận được gói.
		Các hành động xử lý của TOE khi gói tin khớp luật (ví dụ: cho phép, chặn, gửi lệnh thiết lập lại...).
IPS_SBD_EXT.2.1 (tùy chọn)	Kiểm tra các gói tin được đóng gói theo các phương thức khác nhau.	Phương pháp đóng gói.
IPS_SBD_EXT.2.2 (tùy chọn)	Lỗi khi lắp ghép lại các gói tin bị phân mảnh.	Địa chỉ IP nguồn và đích.
		Giao diện TOE đã nhận được các phân mảnh.
IPS_SBD_EXT.2.3 (tùy chọn)	Chuẩn hóa lưu lượng mạng bởi TOE.	Địa chỉ IP nguồn và đích của các gói bị loại bỏ.
		Giao diện của TOE đã nhận các gói tin.

Hoạt động	Hoạt động đảm bảo
TSS	Đánh giá viên kiểm tra TSS có mô tả cách TOE được thiết lập cấu hình để ghi lại các dữ liệu IPS liên quan đến các chính sách áp dụng. Đánh giá viên kiểm tra TSS có mô tả những loại sự kiện IPS (tương tự) nào sẽ kết hợp với bản tin kiểm toán cùng với các điều kiện (ví dụ, ngưỡng, khoảng thời gian). TSS cũng có mô tả mức độ cấu hình có liên quan. Đối với IPS_SBD_EXT.1, cho mỗi trường, đánh giá viên xác minh TSS mô tả cách thức các trường được kiểm tra như thế nào và, nếu không có ghi log, các cơ chế khác như đếm được triển khai.
AGD	Đánh giá viên kiểm tra tài liệu hướng dẫn có mô tả cách thức cấu hình TOE để tạo ra dữ liệu kiểm toán. Đánh giá viên kiểm tra tài liệu hướng dẫn có chỉ dẫn cách cấu hình để ghi lại các sự kiện tương tự (ví dụ: thiết lập các ngưỡng, xác định các cửa sổ thời gian...).
Đánh giá	Đánh giá viên kiểm tra IPS có tạo ra các dữ liệu kiểm toán khi thiết lập các luật, các chính sách và được áp dụng vào các giao diện cảm biến của IPS hay không? Các luật và chính sách phải được thiết lập phù hợp theo kịch bản kiểm thử để có thể tạo ra dữ liệu kiểm toán.

9.2.2 FMT: Quản lý an toàn

9.2.2.1 FMT_SMF.1/IPS Đặc tả chức năng quản lý an toàn (IPS)

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

- Kích hoạt, vô hiệu các luật áp dụng cho từng giao diện của cảm biến và quyết định các hành vi của chức năng IPS.

- Sửa đổi các thông số quyết định lưu lượng mạng được thu thập và phân tích:

- *Địa chỉ IP nguồn (địa chỉ host và địa chỉ mạng)*
- *Địa chỉ IP đích (địa chỉ host và địa chỉ mạng)*
- *Cổng nguồn (TCP và UDP)*
- *Cổng đích (TCP và UDP)*
- *Giao thức (IPv4 và IPv6)*
- *Giao thức ICMP và các mã của giao thức*

- Cập nhật (nhập) luật

- Tạo luật tùy biến

- Phát hiện dị thường

- Kích hoạt và vô hiệu hóa hành động của IPS khi phát hiện tấn công theo luật hoặc dấu hiệu dị thường.

- Thay đổi ngưỡng kích hoạt phản ứng IPS

- Thay đổi thời gian khóa nguồn tấn công

- Cập nhật danh sách IP sạch và danh sách IP đen.

- Thiết lập cấu hình để các danh sách này có thể ghi đè/ưu tiên hơn các luật của IPS.

Hoạt động	Hoạt động đảm bảo
TSS	Đánh giá viên kiểm tra TSS có mô tả việc IPS thực hiện phân tích dữ liệu và thực hiện các hành động được cấu hình thế nào. Lưu ý là các mô tả này phải phù hợp với các hoạt động đảm bảo cho IPS_ABD_EXT.1, IPS_IPB_EXT.1 và IPS_ABD_EXT.1
AGD	Đánh giá viên kiểm tra tài liệu hướng dẫn có mô tả các chức năng an toàn, mô tả cách thiết lập cấu hình mặc định và cách thiết lập các cơ chế khớp luật và các hành động của IPS khi khớp luật.
Đánh giá	Đánh giá viên thực hiện theo các bước sau: **Đánh giá 1:** Đánh giá viên tạo luật và áp dụng vào giao diện cảm biến của IPS. Đánh giá viên tạo dữ liệu kiểm thử và kiểm tra xem IPS có cảnh báo cùng với hành

	động tương ứng thiết lập theo luật hay không? **Đánh giá 2:** Thực hiện vô hiệu hóa luật và tạo dữ liệu kiểm thử như ở trên xem có xuất hiện cảnh báo và hành động của IPS như bước ở trên hay không? **Đánh giá 3:** Thực hiện tải luật từ các nguồn bên ngoài và thực hiện kiểm thử lại như **đánh giá** 1 và 2. Chú ý kiểm thử với các chức năng khác phải khớp với Hoạt động đảm bảo IPS_ABD_EXT.1, IPS_SBD_EXT.1.

9.2.3 IPS: Ngăn chặn xâm nhập

9.2.3.1 IPS_ABD_EXT.1 Chức năng phát hiện dị thường

IPS_ABD_EXT.1.1 TSF hỗ trợ các định nghĩa [lựa chọn (một hoặc nhiều phương án sau): Thông số bình thường, dị thường, đặc điểm kết nối mạng] bao gồm: [lựa chọn:

- Thông lượng *([chỉ định: thông số dữ liệu (ví dụ như byte, các gói dữ liệu,...) khoảng thời gian (ví dụ phút, giờ, ngày)]);*
- Thời gian trong ngày;
- Tần số;
- Ngưỡng;
- *[chỉ định: các phương pháp khác]]*

và theo các trường của giao thức mạng như sau:

- *[lựa chọn: tất cả các tiêu đề và nội dung gói tin tại IPS_SBD_EXT.1; [chỉ định: tập hợp con danh sách các tiêu đề gói tin và dữ liệu các yếu tố từ IPS_SBD_EXT.1]]*

Chú thích áp dụng: Thông số bình thường là những định nghĩa về các thông số của lưu lượng mạng bình thường (IPS_ABD_EXT.1.3) trong khi lưu lượng bất thường là định nghĩa được quy định trong IPS_ABD_EXT.1.3. Tần số có thể được định nghĩa là một số lần xuất hiện của một sự kiện (chẳng hạn như phát hiện số lượng các gói tin khớp luật của IPS) trong khoảng thời gian xác định thời gian, chẳng hạn như số phiên FTP mới trong 1 giờ. Mô tả TSS phải có giải thích về cách thiết lập giá trị tần số trên TOE. Tham số Ngưỡng có thể được định nghĩa độ lệch hoặc tỷ lệ phần trăm độ lệch so với mức thiết lập ban đầu.

IPS_ABD_EXT.1.2 TSF cho phép định nghĩa các hoạt động dị thường thông qua [lựa chọn: cấu hình thủ công/ cấu hình tự động bởi người quản trị].

Chú thích áp dụng: Các thông số "bình thường" và "dị thường" có thể thiết lập bởi một quản trị TOE (hoặc định nghĩa nhập khẩu) hoặc thiết lập tự động bằng cách kiểm tra lưu lượng mạng qua một khoảng thời gian (hay còn gọi là "hồ sơ").

IPS_ABD_EXT.1.3 TSF cho phép thực hiện các hành động sau khi phát hiện dị thường:

- Với bất kỳ chế độ hoạt động, đối với bất kỳ giao diện của cảm biến: [lựa chọn:

  - Cho phép kết nối
  - Gửi gói tin reset đến địa chỉ nguồn vi phạm;
  - Gửi gói tin reset đến địa chỉ đích vi phạm;
  - Gửi gói tin ICMP unreachable [lựa chọn: IP nguồn, IP đích, cổng];
  - Gửi lệnh tương tác tới thiết bị mạng để ngăn chặn tấn công]

- Đối với chế độ nội tuyến:

  - Cho phép kết nối
  - Khóa/hủy bỏ kết nối mạng
  - Và [lựa chọn: thay đổi nội dung gói tin và chuyển tiếp tới đích]

Hoạt động	Hoạt động đảm bảo
TSS	Đánh giá viên kiểm tra TSS có mô tả thành phần, cách xây dựng và áp dụng các tham số bình thường hoặc các thuộc tính dựa trên dị thường trong IPS_ABD_EXT.1.1. Đánh giá viên kiểm tra TSS có mô về cách thức định nghĩa và thiết lập các thông số bình thường trên IPS hoặc mô tả về cách thiết lập các luật để phát hiện dị thường bởi quản trị viên. Đánh giá viên kiểm tra các luật phát hiện dị thường có đưa ra các hành động tương ứng của IPS trong IPS_ABD_EXT.1.3 hay không. Đánh giá viên kiểm tra TSS có mô tả các giao diện của IPS có thể áp dụng các luật phát hiện dị thường và giải thích làm sao có thể áp dụng các giao diện mạng khác của IPS. Trường hợp các giao diện được nhóm lại thành một nhóm thì chúng có thể được coi chung là một giao diện logic riêng biệt.
AGD	Đánh giá viên kiểm tra tài liệu hướng dẫn có chỉ dẫn các lệnh để thiết lập các tham số bình thường và luật phát hiện dị thường theo IPS_ABD_EXT.1.1. Chú ý chức năng tự động thiết lập tham số không nằm trong phạm vi của tiêu chuẩn này. Đánh giá viên kiểm tra tài liệu hướng dẫn có chỉ dẫn lệnh để chỉ ra hành động của IPS kết hợp với luật phát hiện dị thường chỉ ra tại IPS_ABD_EXT.1.3 và đối với các chính sách khác nhau ở các mạng khác nhau.
Đánh giá	Đánh giá viên thực hiện theo các đánh giá sau: Đánh giá 1: Đánh giá viên sử dụng các lệnh theo hướng dẫn để thiết lập tham số bình thường và luật phát hiện dị thường theo IPS_ABD_EXT.1.1. Người quản trị tạo dữ liệu kiểm thử để đánh giá chức năng phát hiện dị thường cùng hành động của IPS khi

	phát hiện dị thường tại IPS_ABD_EXT.1.1. Đánh giá 2: Lặp lại bước đánh giá ở trên đối với các giao diện khác nhau của IPS và với các mạng khác nhau.

9.2.3.2 IPS_IPB_EXT.1 Chức năng chặn địa chỉ IP

IPS_IPB_EXT.1.1: TSF hỗ trợ thiết lập cấu hình danh sách địa chỉ IP sạch và danh sách đen theo [lựa chọn: nguồn, đích] của địa chỉ IP.

Chú thích áp dụng: Các loại địa chỉ quy định tại SFR này các dạng địa chỉ IP (ví dụ như một địa chỉ IP hoặc một dải địa chỉ IP) vì trong tiêu chuẩn này chỉ đề cập tới việc phân tích lưu lượng của giao thức mạng IP. Tuy nhiên việc IPS có thể hỗ trợ phân tích các giao thức khác là tùy chọn, nhưng tài liệu mô tả TSS và hướng dẫn phải giải thích việc cấu hình danh sách các địa chỉ không phải của giao thức IP và danh sách này có mức ưu tiên thấp hơn so với danh sách địa chỉ theo giao thức IP.

IPS_IPB_EXT.1.2: TSF cho phép người quản trị IPS khác nhau có vai trò/quyền khác nhau trong việc thiết lập danh sách các địa chỉ IP cùng với luật sử dụng danh sách địa chỉ IP đó.

Hoạt động	Hoạt động đảm bảo
TSS	Đánh giá viên kiểm tra xem các danh sách địa chỉ IP ảnh hưởng như thế nào đến việc phân tích lưu lượng đối với các gói tin xử lý. TSS phải mô tả chi tiết các thuộc tính đối với các danh sách địa chỉ IP được tạo ra, bao gồm cách xác định địa chỉ IP nguồn hoặc đích (ví dụ: một địa chỉ IP hoặc một dải địa chỉ IP). Đánh giá viên kiểm tra TSS mô tả tất cả các vai trò và mức độ truy cập tương ứng cho mỗi vai trò đã được chỉ định trong yêu cầu ở trên.
AGD	Đánh giá viên kiểm tra tài liệu hướng dẫn có chỉ dẫn thực hiện các lệnh để tạo, sửa, xóa các thuộc tính của danh sách địa chỉ IP.
Đánh giá	Đánh giá viên thực hiện các kiểm tra sau: Đánh giá 1: Đánh giá viên thực hiện tạo các danh sách các địa chỉ IP đen theo hướng dẫn (sử dụng một địa chỉ IP, danh sách các IP hoặc một dải địa chỉ IP). Sau đó tạo dữ liệu kiểm thử và quan sát xem những địa chỉ IP thuộc danh sách đen có tự động bị khóa bởi IP hay không? Đánh giá 2: Đánh giá viên thực hiện tạo các danh sách các địa chỉ IP sạch theo hướng dẫn (sử dụng một địa chỉ IP, danh sách các IP hoặc một dải địa chỉ IP). Sau đó tạo dữ liệu kiểm thử và quan sát xem những địa chỉ IP thuộc danh sách đen có tự động cho phép bởi IP hay không? Đánh giá 3: Người quản trị tạo ra các danh sách trắng và đen nhưng có địa chỉ IP trong các danh sách là giống nhau, sau đó tạo dữ liệu kiểm thử và kiểm tra thứ tự ưu tiên khi xử lý các địa chỉ giống nhau trong danh sách khác nhau theo IPS_NTA_EXT.1.1.

9.2.3.3 IPS_NTA_EXT.1 Chức năng phân tích lưu lượng mạng

IPS_NTA_EXT.1.1 TSF thực hiện phân tích các gói tin gửi đến các giao diện cảm biến của IPS để phát hiện các hành vi vi phạm/ tấn công theo các luật được thiết lập trên IPS.

Chú thích áp dụng: Trường hợp IPS có nhiều giao diện cảm biến khác nhau thì có thể thiết lập nhiều chính sách khác nhau cho IPS (mỗi chính sách là tập các luật khác nhau) và có thể áp dụng và các giao diện cảm biến khác nhau của IPS.

Hoạt động	Hoạt động đảm bảo
TSS	Đánh giá viên kiểm tra TSS có mô tả khả năng của IPS trong việc phân tích lưu lượng IP theo thứ tự ưu tiên. TSS phải có mô tả nếu người quản trị thiết lập các chính sách theo thứ tự ưu tiên khác nhau/thứ tự ưu tiên mặc định trên IPS như: danh sách known-good, danh sách known-bad, luật dựa trên hành vi đã biết, và luật dựa trên sự thay đổi bất thường. Các TSS liên quan đến yêu cầu này được đánh giá trong các hoạt động đảm bảo tiếp theo.
AGD	Đánh giá viên kiểm tra xem tài liệu hướng dẫn có mô tả thứ tự mặc định về các mức độ ưu tiên. Nếu thứ tự ưu tiên được thiết lập thì đánh giá viên kiểm tra xem có hướng dẫn cách thiết lập mức độ ưu tiên không?
Đánh giá	Việc đánh giá liên quan đến yêu cầu này được đánh giá trong các hoạt động đảm bảo tiếp theo.

IPS_NTA_EXT.1.2 TSF có khả năng phân tích lưu lượng mạng của các giao thức sau:

- Giao thức Internet (IPv4), RFC 791
- Giao thức Internet phiên bản 6 (IPv6), RFC 2460
- Giao thức bản tin điều khiển Internet phiên bản 4 (ICMPv4), RFC 792
- Giao thức bản tin điều khiển Internet phiên bản 6 (ICMPv6), RFC 2463
- Giao thức điều khiển truyền vận (TCP), RFC 793
- Giao thức dữ liệu người dùng (UDP), RFC 768

Chú thích áp dụng: Việc đưa ra các giao thức theo các ký hiệu RFC ở trên không có nghĩa IPS phải tuân thủ toàn bộ các trường thông tin được mô tả trong RFC mà đây được như là giao thức tham chiếu để áp dụng.

Hoạt động	Hoạt động đảm bảo
TSS	Đánh giá viên kiểm tra các giao thức sau có được hỗ trợ bởi IPS: - IPv4 - IPv6

	- ICMPv4 - ICMPv6 - TCP - UDP Đánh giá viên kiểm tra xem TSS có mô tả về các giao thức mà IPS hỗ trợ có tương thích với các giao thức ở trên hay không.
AGD	Hướng dẫn liên quan đến yêu cầu này được đánh giá trong các hoạt động đảm bảo tiếp theo.
Đánh giá	Kiểm tra liên quan đến yêu cầu này được đề cập trong các hoạt động đảm bảo kiểm tra tiếp theo.

IPS_NTA_EXT.1.3 TSF cho phép giao diện cảm biến có thể nghe ở chế độ promiscuous và nội tuyến và hỗ trợ chỉ định một hoặc nhiều giao diện như "quản lý" để liên lạc giữa các TOE trong và bên ngoài tổ chức mà không đồng thời là giao diện cảm ứng.

- Chế độ promiscuous (nghe thụ động): *[chỉ định: danh sách các loại giao diện];*
- Chế độ nội tuyến (dữ liệu đi qua IPS): *[chỉ định: danh sách các loại giao diện];*
- Chế độ quản lý: *[chỉ định: danh sách các loại giao diện];*
- [Lựa chọn:
    - Giao diện Session-reset-capable: *[chỉ định: danh sách các giao diện của IPS có khả năng hủy kết nối mạng];*
    - *[chỉ định: Các loại giao diện khác];*
    - không có các loại giao diện khác].

Chú thích áp dụng: Giao diện của IPS có thể là các giao diện Ethernet, Gigabit Ethernet... đối với giao diện chạy chế độ promiscuous là giao diện nghe thụ động và không cung cấp bất kỳ chức năng nào của các giao diện mạng thông thường đối với các giao thức ở lớp 2, lớp 3, hoặc chức năng lớp cao hơn của mô hình OSI, vì vậy các dịch vụ mạng không được lắng nghe trên giao diện này, và không có giao thức IP được kích hoạt trên giao diện này. Đối với chế độ nội tuyến cặp giao diện của IPS là cặp giao diện đón và trả lưu lượng mạng đi qua IPS. Giống như giao diện ở chế độ promiscuous, giao diện ở chế độ nội tuyến cũng không thiết lập chức năng của các giao thức ở lớp 2, lớp 3, hoặc chức năng lớp cao hơn của mô hình OSI.

IPS sử dụng giao diện riêng biệt cho mục đích quản trị/quản lý mà có thể được cấu hình như các giao diện thông thường và cho phép quản lý IPS từ xa theo các quy định tại FTP_ITC, và FTP_TRP. TOE. Giao diện thực hiện chức năng hủy kết nối có thể là giao diện cảm biến của giao diện quản trị của IPS. Chức năng hủy phiên kết nối không phải là chức năng bắt buộc đối với các IPS, nhưng là một lựa chọn trong SFR.

Hoạt động	Hoạt động đảm bảo
TSS	Đánh giá viên kiểm tra TSS có mô tả các kiểu giao diện của IPS với các chế độ hoạt động tương ứng (yêu cầu tối thiểu có một giao diện chạy ở chế độ nội tuyến). TSS cũng mô tả giao diện quản lý là khác biệt với giao diện cảm biến.
AGD	Đánh giá viên kiểm tra tài liệu hướng dẫn có chỉ dẫn về cách triển khai từng trường hợp được mô tả trong TSS hay không. Đánh giá viên cũng kiểm tra xem có hướng dẫn áp dụng các chính sách của IPS đối với các giao diện theo mỗi chế độ triển khai. Nếu giao diện quản lý được cấu hình, đánh giá viên kiểm tra xem có hướng dẫn cách cấu hình giao diện quản lý của IPS. Đánh giá viên kiểm tra tài liệu hướng dẫn có giải thích cách cấu hình cho phép IPS có thể gửi lệnh tương tác đến các thiết bị hệ thống. Chú thích: việc cấu hình kênh kết nối bảo mật giữa IPS và thiết bị hệ thống sẽ được đưa ra trong FTP_ITC.1.
Đánh giá	Các bài kiểm tra liên quan đến yêu cầu này giống như các hoạt động đảm bảo đối với các trường hợp giao diện giám sát của IPS hoạt động ở chế độ nội tuyến, ngẫu nhiên và các yêu cầu trong FTP_ITC.1.

9.2.3.4 IPS_SBD_EXT.1 Chức năng phát hiện theo dấu hiệu

IPS_SBD_EXT.1.1 TSF cho phép phân tích thông tin trong phần tiêu đề của gói tin bao gồm các trường thông tin sau:

- IPv4: Phiên bản; Độ dài mào đầu; Độ dài gói; ID; Cờ IP; Phần bù; Thời gian sống (TTL); Giao thức; Kiểm tra mào đầu; Địa chỉ nguồn; Địa chỉ đích; các tùy chọn IP khác và [lựa chọn: Loại dịch vụ (ToS), các trường khác].
- IPv6: Phiên bản; Phân lớp lưu lượng; Nhãn luồng; Độ dài tải; Mào đầu kế tiếp; Giới hạn số chặng; Địa chỉ nguồn; Địa chỉ đích; Mào đầu định tuyến và [lựa chọn: lớp lưu lượng, nhãn lưu lượng, các trường khác].
- ICMP: Loại; Mã; Kiểm tra mào đầu và [lựa chọn: ID, sequence number, [chỉ định: các trường thông tin khác trong tiêu đề ICMP]].
- ICMPv6: Loại; Mã và Kiểm tra mào đầu.
- TCP: Cổng nguồn; Cổng đích; số thứ tự; số báo nhận; Phần bù; Dự phòng; Cờ TCP; Cửa sổ; Kiểm tra; Con trỏ khẩn và các tùy chọn TCP.
- UDP: Cổng nguồn; Cổng đích; Độ dài và Kiểm tra UDP.

Hoạt động	Hoạt động đảm bảo

TSS	Đánh giá viên kiểm tra TSS có mô tả các thành phần của luật bao gồm các trường thông tin trong phần tiêu đề của gói tin hay không? Đánh giá viên kiểm tra mỗi một luật của IPS có thể kết hợp với một hành động được đưa ra trong IPS_SBD_EXT.1.5. Đánh giá viên kiểm tra TSS có mô tả việc các luật có thể áp dụng vào các giao diện mạng khác nhau của IPS. Trường hợp các giao diện được nhóm lại thành nhóm thì chúng được coi là một giao diện logic và có thể áp dụng các luật của IPS đối với giao diện logic đó.
AGD	Đánh giá viên kiểm tra tài liệu hướng dẫn có chỉ dẫn về cách tạo các luật với các tham số đầu vào là các trường thông tin trong phần tiêu đề gói tin hay không, bao gồm: - IPv4: Phiên bản; Độ dài mào đầu; Độ dài gói; ID; Cờ IP; Phần bù; Thời gian sống (TTL); Giao thức; Kiểm tra mào đầu; Địa chỉ nguồn; Địa chỉ đích và các tùy chọn IP khác. - IPv6: Phiên bản; Phân lớp lưu lượng; Nhãn luồng; Độ dài tải; Mào đầu kế tiếp; Giới hạn số chặng; Địa chỉ nguồn; Địa chỉ đích; Mào đầu định tuyến và các tùy chọn địa chỉ nhà. - ICMP: Loại; Mã; Kiểm tra mào đầu và phần còn lại của mào đầu (thay đổi dựa trên loại và mã ICMP). - ICMPv6: Loại; Mã và Kiểm tra mào đầu. - TCP: Cổng nguồn; Cổng đích; số thứ tự; số báo nhận; Phần bù; Dự phòng; Cờ TCP; Cửa sổ; Kiểm tra; Con trỏ khẩn và các tùy chọn TCP. - UDP: Cổng nguồn; Cổng đích; Độ dài và Kiểm tra UDP. Đánh giá viên kiểm tra tài liệu hướng dẫn có chỉ dẫn cách thiết lập hành động tương ứng với từng luật tạo ra trong IPS_SBD_EXT.1.5.
Đánh giá	Đánh giá viên phải thực hiện các phép thử sau đây: Đánh giá 1: Đánh giá viên thực hiện theo hướng dẫn để tạo ra các luật khác nhau tương ứng với mỗi trường thông tin trong tiêu đề của gói tin. Mỗi luật sẽ có kết hợp với một hành động tương ứng trong IPS_SBD_EXT.1.5. Các trường thông tin trong tiêu đề gói tin bao gồm: - IPv4: Phiên bản; Độ dài mào đầu; Độ dài gói; ID; Cờ IP; Phần bù; Thời gian sống (TTL); Giao thức; Kiểm tra mào đầu; Địa chỉ nguồn; Địa chỉ đích và các tùy chọn IP khác. - IPv6: Phiên bản; Phân lớp lưu lượng; Nhãn luồng; Độ dài tải; Mào đầu kế tiếp; Giới hạn số chặng; Địa chỉ nguồn; Địa chỉ đích; Mào đầu định

	tuyến và các tùy chọn địa chỉ nhà. - ICMP: Loại; Mã; Kiểm tra mào đầu và phần còn lại của mào đầu (thay đổi dự trên loại và mã ICMP). - ICMPv6: Loại; Mã và Kiểm tra mào đầu. - TCP: Cổng nguồn; Cổng đích; số thứ tự; số báo nhận; Phần bù; Dự phòng; Cờ TCP; Cửa sổ; Kiểm tra; Con trỏ khẩn và các tùy chọn TCP. - UDP: Cổng nguồn; Cổng đích; Độ dài và Kiểm tra UDP. Đánh giá viên tạo dữ liệu kiểm thử và kết hợp với ứng dụng phân tích gói tin để kiểm tra khả năng khớp luật theo từng trường thông tin của gói tin và hành động kết hợp tương ứng. Đánh giá 2: Thực hiện lại các bước như đánh giá 1 với từng giao diện khác nhau của IPS.

IPS_SBD_EXT.1.2 TSF có khả năng phân tích phần dữ liệu của gói tin (payload), bao gồm:

- Phần dữ liệu của gói tin ICMPv4, thông tin 4 byte đầu tiên phần tiêu đề gói tin.
- Phần dữ liệu của gói tin ICMPv6, thông tin 4 byte đầu tiên phần tiêu đề gói tin.
- Phần dữ liệu của gói tin TCP (thông tin 20 byte phần tiêu đề gói tin), bao gồm:

  i) Các lệnh FTP (truyền tệp tin): help, noop, stat, syst, user, abort, acct, allo, appe, cdup, cwd, dele, list, mkd, mode, nlst, pass, pasv, port, pass, quit, rein, rest, retr, rmd, rnfr, rnto, site, smnt, stor, stou, stru và type.

  ii) Các lệnh HTTP (web) và các nội dung: các lệnh bao gồm GET và POST, và các chuỗi định nghĩa bởi người quản trị để so khớp URL/URI và nội dung trang web.

  iii) Trạng thái SMTP (thư điện tử): trạng thái start, trạng thái các dòng lệnh SMTP, trạng thái tiêu đề thư điện tử, trạng thái nội dung thư điện tử, trạng thái hủy thư điện tử.

  iv) [lựa chọn: *[chỉ định: các cách kiểm tra phần dữ liệu gói tin TCP khác]*;
- Phần dữ liệu của gói tin UDP, thông tin 8 byte đều tiên phần tiêu đề gói tin.

Thêm nữa, TSF phải hỗ trợ chức năng phân tích các gói tin bị phân mảnh.

Hoạt động	Hoạt động đảm bảo
TSS	Đánh giá viên kiểm tra TSS có mô tả khả năng phân tích nội dung gói tin theo chuỗi ký tự. Đánh giá viên kiểm tra mỗi luật được tạo ra để khớp chuỗi ký tự có thể kết hợp với hành động trong IPS_SBD_EXT.1.5.
AGD	Đánh giá viên kiểm tra tài liệu hướng dẫn có chỉ dẫn cách tạo các luật có tùy chọn khớp

	chuỗi ký tự trọng phần dữ liệu của gói tin trong IPS_SBD_EXT.1.2. Hướng dẫn hoạt động sẽ cung cấp hướng dẫn cấu hình, nếu cần, để phát hiện tải trọng trên nhiều gói tin và khả năng phân tích dữ liệu của gói tin của chuỗi các gói tin. Đánh giá viên kiểm tra khả năng kết hợp với từng hành động trong IPS_SBD_EXT.1.5. Đánh giá viên kiểm tra khả năng áp dụng luật trên các giao diện khác nhau của IPS.
Đánh giá	Đánh giá viên phải thực hiện các phép thử sau đây: Đánh giá 1: Đánh giá viên thực hiện các chỉ dẫn trong hướng dẫn hoạt động để kiểm tra các quy tắc phát hiện dựa trên chuỗi tải trọng gói có thể được gán cho các phản ứng được chỉ định trong IPS_SBD_EXT.1.5 sử dụng các thuộc tính được chỉ định trong IPS_SBD_EXT.1.2. Tuy nhiên không bắt buộc (cũng không khả thi) để kiểm tra tất cả các chuỗi dữ liệu có thể có của chương trình, đánh giá viên phải đảm bảo lựa chọn các chuỗi trong yêu cầu được chọn để được kiểm tra. Tối thiểu ít nhất một chuỗi sử dụng mỗi thuộc tính sau đây từ IPS_SBD_EXT.1.2 nên được kiểm tra cho mỗi giao thức. Đánh giá viên sẽ tạo ra các gói phù hợp với chuỗi trong quy tắc và quan sát phản ứng tương ứng như được định cấu hình. - Phần dữ liệu của gói tin ICMPv4, thông tin 4 byte đầu tiên phần tiêu đề gói tin. - Phần dữ liệu của gói tin ICMPv6, thông tin 4 byte đầu tiên phần tiêu đề gói tin. - Phần dữ liệu của gói tin TCP (thông tin 20 byte phần tiêu đề gói tin), bao gồm: i) Các lệnh FTP (truyền tệp tin): help, noop, stat, syst, user, abort, acct, allo, appe, cdup, cwd, dele, list, mkd, mode, nlst, pass, pasv, port, pass, quit, rein, rest, retr, rmd, rnfr, rnto, site, smnt, stor, stou, stru và type. ii) Các lệnh HTTP (web) và các nội dung: các lệnh bao gồm GET và POST, và các chuỗi định nghĩa bởi người quản trị để so khớp URL/URI và nội dung trang web. iii) Trạng thái SMTP (thư điện tử): trạng thái start, trạng thái các dòng lệnh SMTP, trạng thái tiêu đề thư điện tử, trạng thái nội dung thư điện tử, trạng thái hủy thư điện tử. iv) [lựa chọn: [*chỉ định: các cách kiểm tra phần dữ liệu gói tin TCP khác*]; - Phần dữ liệu của gói tin UDP, thông tin 8 byte đều tiên phần tiêu đề gói tin. Đánh giá 2: Đánh giá viên sẽ lặp lại các kiểm tra trong đánh giá 1 nhưng thực hiện với các gói tin bị phân mảnh. Đánh giá 3: Thực hiện các đánh giá 1 và 2 nhưng áp dụng với các giao diện khác nhau của IPS.

IPS_SBD_EXT.1.3: TSF có khả năng để phát hiện các dấu hiệu dựa trên tiêu đề (sử dụng các trường được xác định trong IPS_SBD_EXT.1.1) tại giao diện cảm ứng IPS:

a) Tấn công địa chỉ IP

i) Lặp gói tin phân mảnh (tấn công Teardrop, tấn công Bonk, hoặc tấn công Boink)

ii) Địa chỉ IP nguồn và đích trùng nhau (tấn công LAND)

b) Tấn công ICMP

i) Phân mảnh lưu lượng ICMP (Ví dụ: tấn công Nuke)

ii) Kích thước gói tin ICMP quá lớn (tấn công Ping of Death)

c) Tấn công TCP

i) Các cờ TCP NULL

ii) Các cờ TCP SYN+FIN

iii) Các cờ TCP FIN

iv) Các cờ TCP SYN+RST

d) Tấn công UDP

i) Tấn công UDP Bomb

ii) Tấn công UDP Chargen DoS

Hoạt động	Hoạt động đảm bảo
TSS	Đánh giá viên kiểm tra TSS có mô tả các cuộc tấn công được định nghĩa trong IPS_SBD_EXT.1.3 được xử lý bởi TOE và phản ứng nào được kích hoạt khi các cuộc tấn công này được xác định.
AGD	Đánh giá viên kiểm tra tài liệu hướng dẫn có chỉ dẫn về các quy tắc cấu hình để xác định các cuộc tấn công được định nghĩa trong IPS_SBD_EXT.1.3 cũng như các phản ứng đối với các cuộc tấn công này như được chỉ định trong IPS_SBD_EXT.1.5.
Đánh giá	Đánh giá 1: Đánh giá viên tạo các luật khác nhau để phát hiện các dạng tấn công khác nhau được mô tả trong IPS_SBD_EXT.1.3. Đối với mỗi dạng tấn công, IPS sẽ áp luật đó vào các giao diện cảm biến khác nhau của IPS và kiểm tra hành động tương ứng trong IPS_SBD_EXT.1.5.

IPS_SBD_EXT.1.4: TSF có khả năng phân tích dòng lưu lượng mạng kết hợp với dấu hiệu của từng gói tin để phát hiện các dạng tấn công mạng sau:

a) Flooding a host (Tấn công DoS)

i) ICMP flooding (Tấn công Smurf, và ping flood)

ii) TCP flooding (Ví dụ: SYN flood)

b) Flooding a network (Tấn công DoS)

c) Quét giao thức và cổng

i) Quét giao thức IP

ii) Quét cổng TCP

iii) Quét cổng UDP

iv) Quét giao thức ICMP

Chú thích áp dụng: Yêu cầu đối với SFR ở trên là yêu cầu tối thiểu đối với IPS để có thể phân tích các trường thông tin của tiêu đề gói tin, chuỗi ký tự trong phần dự liệu của gói tin cũng như luồng dữ liệu để phát hiện các dạng tấn công ở trên.

Đối với một số dạng tấn công dò quét cổng thì đích quét có thể bao gồm nhiều địa chỉ IP khác nhau, các tham số trong gói tin dò quét và thời gian đến giữa các gói tin dò quét có thể là ngẫu nhiên.

Thông thường các IPS thường thiết lập trước các tập luật. Tuy nhiên để có thể phát hiện các dạng tấn công khác IPS cần cho phép tạo các luật tùy biến do người quản trị thiết lập.

Hoạt động	Hoạt động đảm bảo
TSS	Đánh giá viên kiểm tra TSS có mô tả IPS làm thế nào để có thể phát hiện các dạng tấn công mô tả trong IPS_SBD_EXT.1.4 và IPS có khả năng đưa ra những hành động tương ứng nào.
AGD	Đánh giá viên kiểm tra tài liệu hướng dẫn có chỉ dẫn cách thiết lập các luật để phát hiện các dạng tấn công mô tả trong IPS_SBD_EXT.1.4 và cũng như các hành động tương ứng mô tả trong IPS_SBD_EXT.1.5.
Đánh giá	Đánh giá 1: Đánh giá viên tạo các luật khác nhau để phát hiện các dạng tấn công khác nhau được mô tả trong IPS_SBD_EXT.1.4. Đối với mỗi dạng tấn công, IPS sẽ áp luật đó vào các giao diện cảm biến khác nhau của IPS và kiểm tra hành động tương ứng trong IPS_SBD_EXT.1.5.

IPS_SBD_EXT.1.5 TSF cho phép thực hiện những hành động sau khi gói tin khớp luật của IPS:

- Khi IPS hoạt động ở bất kỳ chế độ nào: [lựa chọn:

  o Cho phép kết nối;

  o Gửi gói tin hủy kết nối tới nguồn vi phạm;

  o Gửi gói tin hủy kết nối tới đích vi phạm;

  o Gửi một ICMP unreachable;

  o Gửi lệnh ngăn chặn tấn công đến thiết bị mạng, bảo mật]

- Khi hoạt động ở chế độ nội tuyến:

o cho phép kết nối;

o Khóa /hủy kết nối;

o và [lựa chọn: thay đổi nội dung gói tin và gửi về đích, không có hành động khác]

Chú thích áp dụng: Thuật ngữ "tương tác" có thể hiểu là IPS gửi câu lệnh có cấu trúc tới các thiết bị để yêu cầu ngăn chặn tấn công thông qua giao thức mạng IP hoặc các giao thức khác không phải là giao thức IP. Trường hợp các thiết bị tương tác không phải là thiết bị mạng thì các thiết bị này phải nằm trong phạm vi FTP_ITC.1.3. Đối với các thiết bị tương tác là thiết bị mạng thì phải nằm trong phạm vi FTP_ITC.1. Chức năng thay đổi nội dung gói tin trước khi gửi về đích ở đây có thể là thay đổi các thông tin nhạy cảm như số tài khoản, thông tin cá nhân…

9.3 Yêu cầu bảo đảm an toàn

Tiêu chuẩn này không đưa ra thêm các yêu cầu bảo đảm an toàn đã quy định đối với NDPP hoặc FWPP. Điều quan trọng là cần lưu ý một TOE được đánh giá theo tiêu chuẩn này thì cũng đã đánh giá theo các PP cơ sở. Khi đánh giá TOE, cần áp dụng các SAR được xác định cho PP cơ sở.

10 Môi trường thử nghiệm

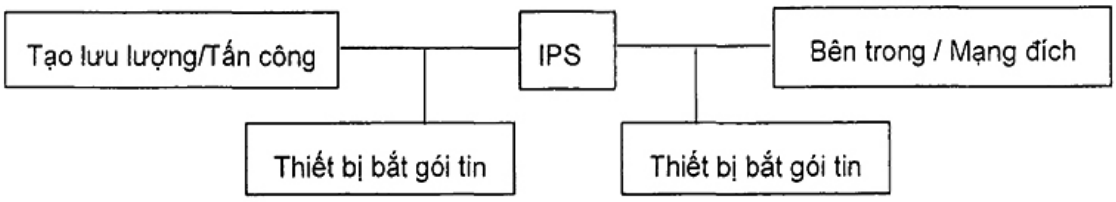
Phần này đưa ra các yêu cầu về môi trường cần bảo đảm để thực hiện các hoạt động đảm bảo ở trên.

Để chuẩn bị môi trường kiểm thử, người quản trị phải có các công cụ để tạo ra các kết nối mạng cũng như việc cho phép tạo ra các gói tin tùy biến, có thể thay đổi các trường thông tin để có thể kiểm thử các chức năng khác nhau của IPS.

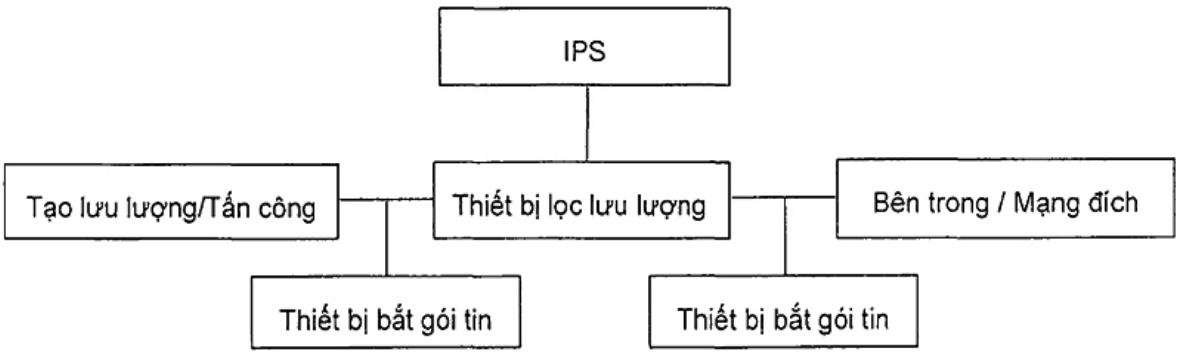
Các kiểm tra ở trên cần phải thực hiện với tất cả với giao diện của IPS. Trong đó, giao diện của IPS có thể hoạt động ở chế độ promiscuous và không được gán địa chỉ IP. Giao diện hoạt động ở chế độ nội tuyến có thể đặt địa chỉ IP hoặc không. Tuy nhiên, giao diện quản trị của IPS phải có địa chỉ IP để kết nối với các thành phần khác trong mạng (như máy chủ syslog, máy chủ AAA, các thiết bị lọc lưu lượng từ xa) và thực hiện chức năng quản trị IPS.

Đánh giá viên tạo ra môi trường kiểm thử tối thiểu đáp ứng yêu cầu như mô hình dưới đây. Đánh giá viên cung cấp các thông tin liên quan đến các môi trường kiểm thử khác nhau. Việc kiểm thử chức năng của IPS có thể triển khai phân tán theo môi trường mạng, phụ thuộc vào các chức năng an toàn được kiểm tra, bao gồm:

- Kiểm tra IPS hoạt động trong mô hình kiểm thử cho chế độ nội tuyến. Trường hợp này, lưu lượng mạng phải đi qua IPS. Nhưng các thành phần khác trong môi trường kiểm thử không nhất thiết phải đón lưu lượng mạng đi qua;
- Kiểm tra IPS hoạt động trong mô hình kiểm thử cho chế độ promiscuous. Trường hợp này, lưu lượng mạng không phải đi qua IPS. Nhưng các thành phần khác trong môi trường kiểm thử không nhất thiết phải đón lưu lượng mạng đi qua.



Hình 2 - Mô hình kiểm tra IPS hoạt động trong mô hình kiểm thử cho chế độ Nội tuyến



Hình 3 - Mô hình kiểm tra IPS hoạt động trong mô hình kiểm thử cho chế độ Promiscuous

Thiết bị IPS có thể được triển khai trên môi trường kiểm thử với nhiều chế độ cùng một lúc. Tuy nhiên đánh giá viên phải thiết lập môi trường kiểm thử phù hợp để có thể thỏa mãn các yêu cầu trong hoạt động kiểm thử.

Việc tạo ra các gói tin với các trường thông tin tùy biến cũng phải cho phép mô phỏng được các dạng tấn công để phục vụ việc kiểm thử. Hệ thống tạo dữ liệu kiểm thử có thể là phần mềm thương mại hoặc phần mềm miễn phí.

Phụ lục A

(Quy định)

Cơ sở đánh giá

Phần này đưa ra các mối đe dọa một cách tổng thể mà IPS cần phải xử lý; các phương pháp sử dụng để giảm thiểu những mối đe dọa và mức độ giảm thiểu có thể đạt được khi sử dụng các thiết bị IPS. Phần này chứa các bảng có thể được sử dụng cho các hoạt động đánh giá trong tài liệu này.

A.1 Định nghĩa các vấn đề về an toàn thông tin

A.1.1 Giả định

Các điều kiện cụ thể được liệt kê dưới đây được cho là đáp ứng môi trường hoạt động của TOE. Những giả định ở đây bao gồm những quy định tại các PP cơ sở và bao gồm các điều kiện trong môi trường thực tiễn trong phát triển các yêu cầu an toàn đối với TOE.

Bảng A-1: Các giả định TOE

Tên giả định	Định nghĩa giả định
A.CONNECTIONS	Giả định rằng IPS được kết nối với các mạng riêng biệt và đảm bảo các chính sách bảo mật thiết lập trên IPS sẽ được thực thi đối với lưu lượng mạng có kết nối với IPS.

A.1.2 Các mối đe dọa

Các mối đe dọa được liệt kê dưới đây được xử lý bằng cách sử dụng thiết bị IPS. Lưu ý rằng nếu FWPP đưa ra các mối đe dọa cần phải xử lý trong PP cơ sở thì trong những trường hợp này, các mối đe dọa chung giống nhau sẽ được sử dụng chung cho chức năng tường lửa và chức năng IPS.

Bảng A-2: Các mối đe dọa

Tên mối đe dọa	Định nghĩa mối đe dọa
T.NETWORK_DISCLOSURE	Lộ lọt thông tin nhạy cảm, bí mật trên môi trường mạng.
T. NETWORK_ACCESS	Truy cập trái phép dịch vụ từ bên ngoài hoặc bên trong mạng. Ví dụ như việc truy cập, điều khiển các thiết bị trong hệ thống mạng thông qua các phần mềm độc hại, cửa hậu.
T.NETWORK_MISUSE	Việc tin tặc thực hiện các hình thức tấn công vào các dịch vụ được cung cấp bởi hệ thống từ các mạng bên ngoài. Thông qua các dịch vụ công cộng này tin tặc có thể thực hiện các hình thức tấn công mạng như: chèn câu truy vấn độc hại SQL, lừa đảo, buộc hủy kết nối, mã độc trong tệp tin nén, tệp tin ngụy trang, chiếm quyền điều khiển, và các mạng botnet.

T.NETWORK_DOS	Tấn công vào những dịch vụ/hệ thống được cung cấp bởi hệ thống, gây lên việc các dịch vụ bị cạn kiệt tài nguyên, quá tải và làm gián đoạn hoạt động của dịch vụ/hệ thống. Mặc dù hầu hết các IPS sẽ cung cấp chức năng bảo vệ tấn công từ chối dịch vụ phân tán DDoS, nhưng chức năng này không phải là bắt buộc đối với IPS. Tuy nhiên chức năng phòng chống tấn công DoS là bắt buộc.

A.1.3 Chính sách bảo mật của tổ chức

Tổ chức triển khai TOE kỳ vọng được đáp ứng các chính sách bảo mật của tổ chức mình như liệt kê dưới đây. Những mục tiêu an toàn này là bổ sung thêm từ PP cơ sở.

Bảng A-3: Chính sách

Tên chính sách	Định nghĩa chính sách
P.ANALYZE	Các quy trình phân tích và thông tin để đưa ra kết luận về những hành vi xâm nhập tiềm tàng phải được xử lý bởi IPS và các hành động ứng phó thích hợp.

A.1.4 Định nghĩa các vấn đề an toàn tương quan

Bảng dưới đây ánh xạ các mối đe dọa, giả định, và các chính sách an toàn tổ chức (OSP) định nghĩa trong tiêu chuẩn này để các mục tiêu an toàn.

Bảng A-4: Định nghĩa các vấn đề an toàn tương quan

Mối đe dọa, Giả định hoặc các chính sách an toàn tổ chức	Mục tiêu an toàn
A.CONNECTIONS	OE.CONNECTIONS
T.NETWORK_DISCLOSURE	O.SYSTEM_MONITORING O.IPS_ANALYSE, O.IPS_REACT
T. NETWORK_ACCESS	O.SYSTEM_MONITORING, O.IPS_ANALYSE, O.IPS_REACT
T.NETWORK_MISUSE	O.SYSTEM_MONITORING, O.IPS_ANALYSE, O.IPS_REACT
T.NETWORK_DOS	O.SYSTEM_MONITORING, O.IPS_ANALYSE, O.IPS_REACT
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS (từ PP cơ sở)	O.TOE_ADMINISTRATION
T.UNSTRUSTED_COMMUNICATION_CHANNELS (từ PP cơ sở)	O.TRUSTED_COMMUNICATIONS (tùy chọn)
P.ANALYZE	O.IPS_ANALYZE, O.TOE_ADMINISTRATION

A.2 Các mục tiêu an toàn

A.2.1 Các mục tiêu an toàn cho TOE

Bảng dưới đây mô tả các mục tiêu an toàn cho TOE. Một TOE đáp ứng các yêu cầu trong tiêu chuẩn này sẽ đáp ứng các mục tiêu an toàn sau:

Bảng A-5: Mục tiêu An toàn cho TOE

Mục tiêu an toàn	Định nghĩa mục tiêu an toàn
O.SYSTEM_MONITORING	IPS thu thập và lưu trữ thông tin về tất cả các sự kiện vi phạm chính sách, các truy cập trái phép hoặc hoạt động độc hại trên mạng được ghi nhận.
O.IPS_ANALYZE	IPS phân tích và xử lý thông tin để phát hiện các hành động xâm nhập và vi phạm chính sách của hệ thống.
O.IPS_REACT	IPS phải có chức năng xử lý các hành vi vi phạm chính sách phát hiện được tới người quản trị hệ thống theo các chính sách/luật được thiết lập trước.
O.TOE_ADMINISTRATION	IPS phải cung cấp chức năng cho phép người quản trị có thể quản trị IPS để quản lý, giám sát hoạt động và thiết lập các chính sách/luật cho IPS.
O.TRUSTED_COMMUNICATIONS	IPS phải cung cấp kênh kết nối tin cậy để cho phép IPS có thể giao tiếp với các thành phần khác trong hệ thống an toàn.

A.2.2 Mục tiêu an toàn cho môi trường hoạt động

Bảng dưới đây chứa các mục tiêu an toan cụ thể đối với môi trường hoạt động của các thiết bị IPS. Những mục tiêu an toàn này là bổ sung thêm từ PP cơ sở.

Bảng A-6: Mục tiêu an toàn cho môi trường kiểm thử

Mục tiêu an toàn	Định nghĩa mục tiêu an toàn
OE.CONNECTIONS	Các quản trị viên đảm bảo rằng TOE được cài đặt phù hợp để cho phép TOE thực thi hiệu quả các chính sách của hệ thống.

A.2.3 Các mục tiêu an toàn tương ứng

Sự tương ứng giữa yêu cầu chức năng an toàn (SFR) và mục tiêu an toàn được đưa ra trong điều 8 của tiêu chuẩn này.

A.3 Tính phù hợp cho các yêu cầu an toàn

Bảng A-7: Tính phù cho yêu cầu quy định rõ ràng

SFR	Lý do
IPS_ABD_EXT.1	SFR này được tạo ra để cho phép TOE có thể phân tích và xử lý với các hoạt động dị thường phát hiện được trên môi trường mạng.
IPS_IPB_EXT.1	SFR này được tạo ra để cho phép TOE có thể tạo và quản lý danh sách trắng và danh sách đen đối với địa chỉ IP để tối ưu hóa khả năng xử lý của TOE bằng cách phân tích lưu lượng truy cập dựa trên các luật của IPS.
IPS_NTA_EXT.1	SFR này được tạo ra để cho phép TOE phân tích lưu lượng mạng và giao thức mạng sử dụng hai phương pháp dựa trên chữ ký và phát hiện dị thường.
IPS_SBD_EXT.1	SFR này được tạo ra để cho phép TOE có thể phân tích và phát hiện xâm nhập dựa theo tập luật và có thể đưa ra các hành động khi phát hiện xâm nhập trên môi trường mạng.
IPS_SBD_EXT.2	SFR này được tạo ra để cho phép TOE có thể tái tạo lại các gói tin bị phân mảnh và cho phép IPS có thể phân tích lưu lượng mạng trong đó có các gói tin bị phân mảnh.

Bảng A-8: Tính phù hợp cho SFR phụ thuộc

SFR	Sự phụ thuộc	Lý do
FAU_ARP.1	FAU_SAA.1	Ngoài ra đáp ứng bởi lớp IPS yêu cầu mở rộng (xác định hành vi được đánh dấu là "vi phạm bảo mật tiềm ẩn" trong FAU_ARP.1.1).
FAU_GEN.1/IPS	FPT_STM.1	Sử dụng trong PP cơ sở.
FAU_SAR.1	FAU_GEN.1	Đưa ra trong tiêu chuẩn này (như FAU_GEN.1/IPS lặp lại).
FAU_SAR.2	FAU_SAR.1	Đưa ra trong tiêu chuẩn này.
FAU_SAR.3	FAU_SAR.1	Đưa ra trong tiêu chuẩn này.
FAU_STG.1	FAU_GEN.1	Đưa ra trong tiêu chuẩn này (như FAU_GEN.1/IPS lặp lại).
FAU_STG.4	FAU_STG.1	Đưa ra trong tiêu chuẩn này.
FMT_MOF.1/IPS	FMT_SMF.1	Phân cấp từ SFR (như FMT_SMR.2/IPS lặp lại).
	FMT_SMR.1	Đưa ra trong tiêu chuẩn này (như

		FMT_SMF.1/IPS lặp lại).
FMT_SMF.1/IPS	Không phụ thuộc.	Không áp dụng.
FMT_SMR.2/IPS	FIA_UID.1	Thay thế bởi FIA_UIA_EXT.1 và kế thừa từ PP cơ sở (đưa chức năng định danh và xác thực trên cùng một SFR).
FPT_FLS.1/Nội tuyến	Không phụ thuộc	Không áp dụng.
FPT_ITT.1	Không phụ thuộc..	Không áp dụng.
FRU_RSA.1	Không phụ thuộc.	Không áp dụng.
IPS_ABD_EXT.1	Không phụ thuộc.	Không áp dụng.
IPS_IPB_EXT.1	Không phụ thuộc.	Không áp dụng.
IPS_NTA_EXT.1	Không phụ thuộc.	Không áp dụng.
IPS_SBD_EXT.1	Không phụ thuộc.	Không áp dụng.
IPS_SBD_EXT.2	IPS_SBD_EXT.1	Đã được bao gồm trong tiêu chuẩn.

Phụ lục B

(Quy định)

Các yêu cầu tùy chọn

Các yêu cầu cơ bản có trong nội dung của tiêu chuẩn này. Ngoài ra, có thêm ba loại khác được yêu cầu quy định tại Phụ lục B, C và D.

Loại thứ nhất (tại Phụ lục B) là yêu cầu mà có thể được bao gồm trong ST, nhưng không phải bắt buộc để TOE xác nhận sự phù hợp với tiêu chuẩn này. Loại thứ hai (tại Phụ lục C) là yêu cầu dựa trên các yêu cầu lựa chọn trong nội dung của tiêu chuẩn này: các yêu cầu nếu lựa chọn trong phần nội dung tiêu chuẩn thì các yêu cầu tương ứng trong Phụ lục C phải được sử dụng để đánh giá sản phẩm. Loại thứ ba (trong Phụ lục D) là các yêu cầu không bắt buộc trong tiêu chuẩn này, nhưng được khuyến khích sử dụng để đánh giá sản phẩm IPS. Lưu ý rằng tác giả ST cần đảm bảo rằng các yêu cầu có liên quan đến yêu cầu trong Phụ lục B, Phụ lục C, và Phụ lục D không được liệt kê (ví dụ, các yêu cầu FMT-type) cũng được bao gồm trong ST.

B.1 Yêu cầu

Các yêu cầu chức năng an toàn tùy chọn được nêu trong phần dưới đây.

B.1.1 FAU: Kiểm toán an toàn

Thuật ngữ "dữ liệu IPS" bao gồm tất cả các dữ liệu được trích xuất từ lưu lượng mạng và lưu trữ trên TOE; các kết quả phân tích được thực hiện bởi TOE và các thông báo cho biết phản ứng của TOE đối với phân tích đó. Định nghĩa "dữ liệu IPS" loại trừ "dữ liệu kiểm toán" đề cập trong PP cơ sở, bao gồm dữ liệu xác định tại FAU_GEN trong PP cơ sở, chẳng hạn như xác thực của các người quản trị, và việc thiết lập/chấm dứt các kênh tin cậy. Nếu việc lưu trữ và/hoặc rà soát dữ liệu IPS và báo động an toàn được hỗ trợ bởi TOE thì các yêu cầu kiểm toán sau đây có thể được bao gồm trong ST.

B.1.1.5 FAU_STG.1 Bảo vệ lưu trữ dấu vết kiểm toán (dữ liệu IPS)

FAU_STG.1.1 tinh chỉnh: TSF sẽ bảo vệ ~~các bản ghi kiểm toán~~ **dữ liệu IPS** đã lưu trữ khỏi xóa trái phép.

FAU_STG.1.2 tinh chỉnh: TSF sẽ có thể [*ngăn chặn*] sửa đổi trái phép đối với ~~các bản ghi kiểm toán~~ **dữ liệu IPS** đã lưu trữ ~~trong dấu vết kiểm toán~~.

Chú thích áp dụng: Không có thêm các sự kiện IPS có thể kiểm toán cần phải được đưa vào FAU_GEN.1/IPS.

Hoạt động	Hoạt động bảo đảm
TSS	Đánh giá viên phải đảm bảo rằng TSS xác định cách dữ liệu IPS được bảo vệ khỏi sự sửa đổi và xóa trái phép.
AGD	Đánh giá viên sẽ xác nhận tài liệu hướng dẫn có mô tả cách bảo vệ dữ liệu IPS khỏi sự sửa đổi và xóa trái phép.

Đánh giá	Đánh giá 1: Đánh giá viên phải lập ra các cách kiểm tra chứng minh rằng dữ liệu IPS có thể được bảo vệ khỏi sự sửa đổi và xóa trái phép.

B.1.1.6 FAU_STG.4 Phòng chống mất mát dữ liệu (dữ liệu IPS)

FAU_STG.4.1 tinh chỉnh: TSF **có thể** cho phép: [lựa chọn: "Không tạo các sự kiện cảnh báo của IPS","Ngăn chặn các sự kiện **IPS** có thể kiểm toán, ~~ngoại trừ những trường hợp được cho phép~~", "Ghi đè lên ~~các bản ghi kiểm toán~~ dữ liệu IPS được lưu trữ đã quá cũ"], và [không có các hành động khác] nếu dấu vết ~~kiểm toán~~ **dữ liệu IPS** đầy.

Các sự kiện có thể kiểm toán	**Nội dung bản ghi kiểm toán bổ sung**
Kiểm tra dung lượng lưu trữ đạt đến giới hạn lưu trữ.	Chỉ ra rằng kiểm tra dung lượng lưu trữ đã đầy và (nếu có thể cấu hình) cách TOE phản ứng (ví dụ: lỗi trong việc kiểm toán các sự kiện có thể kiểm toán mới hoặc ngăn các sự kiện có thể kiểm toán xảy ra).

Hoạt động	**Hoạt động bảo đảm**
TSS	Đánh giá viên phải đảm bảo rằng TSS xác định cách đăng nhập dữ liệu IPS được xử lý khi dấu vết kiểm toán dữ liệu IPS đã đầy. TSS cũng sẽ xác định cách ghi lại dữ liệu IPS được khôi phục.
AGD	Đánh giá viên sẽ xác nhận tài liệu hướng dẫn có mô tả các bước liên quan đến quản lý ghi chép dữ liệu IPS khi dấu vết kiểm toán IPS đã đầy.
Đánh giá	Không có hoạt động kiểm tra nào cho yêu cầu này.

B.1.2 FMT: Yêu cầu quản lý an toàn

Nếu TOE cho phép nhiều vai trò quản lý, thì các yêu cầu này có thể được bao gồm trong ST.

B.1.2.1 FMT_MOF.1/IPS Quản lý chức năng an toàn theo hành vi

FMT_MOF.1.1/IPS TSF sẽ hạn chế khả năng [sửa đổi hành vi của] các chức năng [*thu thập, phân tích và phản ứng dữ liệu IPS*] cho [*người quản trị IPS được ủy quyền*].

Hoạt động	**Hoạt động bảo đảm**
TSS	Đánh giá viên phải kiểm tra TSS để xác định rằng, đối với mỗi chức năng quản trị được xác định tài liệu hướng dẫn, chức năng nào có thể truy cập qua một giao diện trước khi người quản trị đăng nhập là được xác định. Đối với mỗi chức năng này, đánh giá viên cũng sẽ xác nhận rằng TSS cho biết chi tiết về khả năng thao tác cấu hình của hệ thống thông qua giao diện này là không được phép đối với người dùng không phải là người quản trị.
AGD	Đánh giá viên xem xét tài liệu hướng dẫn để xác định rằng mỗi chức năng được

	thực hiện để đáp ứng các yêu cầu của tiêu chuẩn này được xác định và thông tin cấu hình được cung cấp để đảm bảo rằng chỉ có người quản trị mới có quyền truy cập vào các chức năng.
Đánh giá	Kiểm tra cho SFR này được hoàn thành như một phần của việc kiểm tra các yêu cầu FMT khác được xác định bởi tiêu chuẩn này.

B.1.2.2 FMT_MTD.1/IPS Quản lý dữ liệu IPS

FMT_MTD.1.1/IPS tinh chỉnh: TSF sẽ hạn chế khả năng [lựa chọn: thay đổi mặc định, truy vấn, chỉnh sửa, xóa, *[chỉ định: các hoạt động khác]]* các [*chỉ định: danh sách các dữ liệu ~~TSF~~ IPS] cho [chỉ định: Người quản trị IPS, Chuyên viên phân tích IPS và các vai trò IPS cụ thể được ủy quyền khác được xác định trong FMT_SMR.2/IPS*].

Chú thích áp dụng: ST nên xác định những vai trò được phép truy cập vào dữ liệu IPS (Người quản trị IPS, Chuyên viên phân tích IPS, và các vai trò IPS cụ thể được ủy quyền khác được xác định trong FMT_SMR.2/IPS). ST có thể xác định bất kỳ số lượng vai trò nào có thể đáp ứng yêu cầu này. Không có thêm sự kiện IPS có thể kiểm toán mà cần phải được bao gồm trong FAU_GEN.1/IPS.

Hoạt động	Hoạt động bảo đảm
TSS	Đánh giá viên phải xác minh rằng TSS bao gồm một mô tả về từng vai trò được xác định liên quan đến trách nhiệm của vai trò và quyền truy cập liên quan đến vai trò đó trên TOE.
AGD	Đánh giá viên sẽ xem xét tài liệu hướng dẫn để đảm bảo rằng nó có các chỉ dẫn để cấu hình các người quản trị được ủy quyền hạn chế khả năng các vai trò xác định đã được ủy quyền chỉ trong các vai trò được ủy quyền.
Đánh giá	Không cần thiết cho tất cả các hoạt động được mô tả trong SFR này có thể truy cập qua tất cả các giao diện TOE. Trong quá trình thực hiện các hoạt động kiểm tra cho việc đánh giá, đánh giá viên sẽ sử dụng tất cả các giao diện áp dụng cho mỗi chức năng quản trị được mô tả trong SFR này mặc dù không cần lặp lại mỗi phép thử liên quan đến hành động quản trị với mỗi giao diện. Đánh giá 1: Đánh giá viên phải chứng minh rằng sau khi cấu hình TOE cho lần sử dụng đầu tiên từ hướng dẫn hoạt động, có thể hạn chế khả năng truy vấn và sửa đổi dữ liệu IPS sử dụng mỗi vai trò được ủy quyền được xác định theo yêu cầu.

B.1.2.3 FMT_SMR.2/Vai trò bảo vệ IPS (IPS)

FMT_SMR.2.1/IPS tinh chỉnh: TSF sẽ duy trì vai trò: [***Người quản trị IPS, Chuyên gia phân tích IPS, và [lựa chọn: [chỉ định: các vai trò IPS được ủy quyền khác], không có vai trò khác***]].

FMT_SMR.2.2/IPS TSF sẽ có thể kết hợp người sử dụng với vai trò.

FMT_SMR.2.3/IPS TSF phải đảm bảo *[chỉ định: điều kiện cho các vai trò khác nhau]* được đáp ứng.

Chú thích áp dụng: Các vai trò được định nghĩa trong SFR này được dự định được cụ thể để quản lý các chức năng IPS. Vai trò "Người quản trị được ủy quyền" được định nghĩa trong PP cơ sở ở FMT_SMR.2 có thể là cùng vai trò là "Người quản trị IPS" được định nghĩa trong tiêu chuẩn này hoặc có thể là một vai trò khác nếu người quản trị được ủy quyền có đầy đủ quyền để quản lý toàn bộ TOE và Người quản trị IPS chỉ có toàn quyền đến chức năng IPS cụ thể. Vai trò Chuyên viên phân tích IPS được thiết kế để đại diện cho một vai trò có ít quyền hơn, hoặc có thể có quyền chỉ cho phép đọc. Các vai trò khác có thể được xác định bởi tác giả ST. Không có thêm các sự kiện IPS có thể kiểm toán nào cần phải được đưa vào FAU_GEN.1/IPS.

Hoạt động	Hoạt động đảm bảo
TSS	Đánh giá viên sẽ xem xét TSS để đảm bảo nó mô tả sự phân biệt giữa các quyền của Người quản trị IPS, Chuyên viên phân tích IPS, và bất kỳ vai trò nào khác được xác định trong chỉ định SFR này. TSS cũng nên mô tả bất kỳ sự phân biệt, nếu có, giữa các quyền của Người quản trị IPS được xác định trong SFR này và Người quản trị được ủy quyền được xác định trong FMT_SMR.2 của PP cơ sở.
AGD	Không có hướng dẫn về hoạt động đảm bảo cho SFR này.
Đánh giá	Do các vai trò quản trị cần phải xem dữ liệu TSF, phân tích được thực hiện bởi đánh giá viên trong hoạt động bảo đảm cho FMT_MTD.1 sẽ chứng minh rằng điều này yêu cầu được đáp ứng.

B.1.3 FPT: Bảo vệ TSF

B.1.3.1 FPT_FLS.1/Inline Lỗi trong duy trì trạng thái an toàn

FPT_FLS.1.1/Inline tinh chỉnh: TSF sẽ **có thể** duy trì một trạng thái an toàn **cho các cổng kết nối nội tuyến** khi lỗi xảy ra: [*chỉ định: danh sách các loại lỗi trong TSF*].

Chú thích áp dụng: Mục đích của SFR này trong tiêu chuẩn là cho phép tác giả ST xác định các loại lỗi có thể xảy ra trên TOE có thể dẫn đến việc không phát hiện có hiệu quả và phản ứng lại các vi phạm chính sách IPS cho lưu lượng đi qua cổng kết nối nội tuyến, và không cho phép lưu lượng đi qua các cổng kết nối này. Tinh chỉnh "có thể" áp dụng để cho phép người quản trị TOE cấu hình TOE cho phép lưu lượng kết nối đi qua các cổng kết nối nội tuyến khi TOE trong tình trạng một phần của lỗi hoàn toàn, nhưng đảm bảo rằng TOE có khả năng chặn lưu lượng nếu nó đã được cấu hình để làm như vậy. Mục đích của SFR này, như đã nêu trong TCVN 8709-2:2011 ISO/IEC 15408-2:2008, là để "đảm bảo rằng TOE sẽ luôn luôn thực thi các SFR của nó trong trường hợp xác định có lỗi trong TSF". Do một số các SFR yêu cầu kiểm tra dữ liệu, và kiểm tra này không thể xảy ra khi một cổng kết nối bị lỗi, sẽ không phải luôn luôn đúng là "tất cả" các SFR sẽ tiếp tục được áp dụng trong trường hợp có lỗi của các thành phần nhất định.

Kiểm tra sự kiện	Nội dung ghi chép kiểm tra bổ sung
Lỗi TSF.	Loại lỗi đã xảy ra.

Hoạt động	Hoạt động bảo đảm
TSS	Đánh giá viên sẽ xem lại phần TSS để xác định rằng việc thực hiện chức năng an toàn khi lỗi của TOE được ghi vào tài liệu. Đánh giá viên đầu tiên sẽ kiểm tra phần TSS để đảm bảo rằng tất cả các chế độ lỗi được chỉ định trong ST được mô tả. Đánh giá viên sau đó sẽ đảm bảo rằng TOE sẽ đạt được trạng thái an toàn sau khi chèn từng loại chế độ lỗi đã chỉ định. Đánh giá viên sẽ xem xét TSS để xác định xem liệu người quản trị TOE có thể lập cấu hình cách truyền lưu lượng đi khi bị tác động bởi những lỗi này.
AGD	Không có hướng dẫn về hoạt động đảm bảo cho SFR này.
Đánh giá	Đối với mỗi loại lỗi được liệt kê trong tài liệu, nhà cung cấp TOE phải cung cấp cho đánh giá viên các phương tiện để kích hoạt lỗii và đánh giá viên phải tái tạo từng loại lỗi để đảm bảo rằng một chính sách IPS áp dụng vẫn được thi hành trong thời gian lỗi. Ví dụ, các nguyên nhân khác nhau bao gồm mất điện tạm thời có thể dẫn đến khởi động lại TOE. Nếu chính sách IPS áp dụng tại thời điểm lỗi (ví dụ như khởi động lại) đảm bảo rằng các gói tin ICMP echo sẽ bị chặn bởi TOE, đánh giá viên sẽ xác nhận rằng không có thời điểm nào trong lúc tắt máy hoặc khởi động lại TOE có bất kỳ gói tin ICMP echo nào được phép thông qua TOE (mặc dù trong ví dụ này, cần hiểu rằng sẽ có một khoảng thời gian mà các sự kiện IPS không được kiểm toán trong lúc cơ chế kiểm toán đang khởi động lại).

B.1.3.2 FPT_ITT.1 Bảo vệ chuyển dữ liệu TSF nội bộ cơ bản

FPT_ITT.1.1 tinh chỉnh: TSF sẽ bảo vệ dữ liệu TSF khỏi [tiết lộ, thay đổi] **sử dụng [lựa chọn: chọn một hoặc nhiều trong số: IPsec, SSH, TLS, HTTPS]** khi nó được chuyển giữa ***[chỉ định: danh sách các thành phần phân tán của TOE]*** ~~các phần riêng biệt của TOE~~.

Chú thích áp dụng: Dựa trên các lựa chọn thực hiện ở đây, một ST tuân thủ sẽ bao gồm một hoặc nhiều SFR dựa trên lựa chọn FCS_IPSEC_EXT.1, FCS_HTTPS_EXT.1, FCS_SSHC_EXT.1, FCS_SSHS_EXT.1, FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, và FCS_TLSS_EXT.2 được quy định tại các PP cơ sở. Một ST tuân thủ cũng sẽ bao gồm mục tiêu tùy chọn O. TRUSTED_COMMUNICATIONS.

Hoạt động	Hoạt động đảm bảo
TSS	Đánh giá viên sẽ kiểm tra TSS để xác định rằng, đối với tất cả các giao tiếp giữa các thành phần TOE phân tán được xác định trong yêu cầu, mỗi cơ chế truyền thông được xác định theo các giao thức được phép cho thành phần đó. Đánh giá viên cũng sẽ xác nhận rằng tất cả các giao thức được liệt kê trong TSS được xác

	định và bao gồm trong các yêu cầu trong ST.
AGD	Đánh giá viên phải xác nhận rằng tài liệu hướng dẫn có chỉ dẫn để thiết lập các giao thức được cho phép với mỗi thành phần TOE, và nó có chứa các chỉ dẫn khôi phục nếu kết nối vô ý bị phá vỡ.
Đánh giá	Đánh giá viên phải thực hiện các phép thử sau đây: Đánh giá 1: Đánh giá viên phải bảo đảm rằng các giao tiếp sử dụng mỗi giao thức với mỗi thành phần TOE được kiểm tra trong quá trình đánh giá, thiết lập các kết nối như mô tả trong tài liệu hướng dẫn và đảm bảo rằng giao tiếp thành công. Đánh giá 2: Đánh giá viên phải đảm bảo, đối với mỗi kênh truyền thông giữa các thành phần phân tán TOE, dữ liệu trên kênh truyền không được gửi bằng bản rõ. Đánh giá 3: Đối với mỗi giao thức gắn với mỗi thành phần TOE được kiểm tra trong suốt bài kiểm tra 1, kết nối sẽ bị gián đoạn về mặt vật lý. Đánh giá viên phải đảm bảo rằng khi kết nối vật lý được khôi phục, việc giao tiếp được bảo vệ hợp lý.

B.1.4 FRU: Tận dụng nguồn tài nguyên

B.1.4.1 FRU_RSA.1 Hạn ngạch tối đa

FRU_RSA.1.1 TSF sẽ thực thi hạn ngạch tối đa các nguồn sau: [*nguồn lực hỗ trợ kiểm tra lưu lượng mạng*] mà [đối tượng] có thể sử dụng [đồng thời].

Chú thích áp dụng: Các TOE tuân thủ sẽ áp đặt hạn ngạch đối với tài nguyên có thể cạn kiệt được sử dụng để hỗ trợ kiểm tra lưu lượng mạng mà "các đối tượng" (các luồng lưu lượng mạng được kiểm tra) có thể sử dụng cùng một lúc. Mục đích của yêu cầu này là để đảm bảo rằng TOE không triển khai theo cách mà các luồng dữ liệu trên cổng kết nối cảm biến của nó có thể vượt quá lưu lượng mà TOE có khả năng kiểm tra. Nếu (dung lượng/tốc độ) dữ liệu của luồng kết nối được kiểm tra vượt quá hạn ngạch được xác định, các TOE nên kích hoạt một cảnh báo biểu thị hạn ngạch đã bị vượt quá, ví dụ: khi TOE được triển khai nội tuyến, vượt hạn ngạch có thể dẫn đến TSF chặn (không chuyển tiếp) và thất bại trong việc kiểm tra lưu lượng mạng; hoặc khi TOE không triển khai nội tuyến, vượt hạn ngạch có thể dẫn đến lưu lượng được chuyển tiếp mà không được kiểm tra. Trong mọi trường hợp, vượt hạn ngạch tối đa sẽ dẫn đến kết quả là một "khả năng vi phạm an toàn" có liên quan đến FAU_ARP ở chỗ TSF có thể đã thất bại trong việc kiểm tra một số lưu lượng mạng.

Sự kiện có thể kiểm toán	**Nội dung bản ghi kiểm toán bổ sung**
Lưu lượng truy cập vượt quá hạn ngạch tối đa.	Đinh danh của giao diện TOE mà đã vượt quá hạn ngạch.

Hoạt động	Hoạt động đảm bảo
TSS	Đánh giá viên phải kiểm tra TSS để đảm bảo rằng nó xác định tất cả các tài nguyên được kiểm soát thông qua cơ chế hạn ngạch và rằng danh sách này chứa các nguồn lực được sử dụng để hỗ trợ kiểm tra lưu lượng mạng. Đánh giá viên phải đảm bảo rằng TSS mô tả cách mỗi tài nguyên được tính là "đã sử dụng" và cách xác định một hạn ngạch hoặc sử dụng tối đa, cũng như các hành động được thực hiện khi đạt đến hạn ngạch.
AGD	Đánh giá viên sẽ kiểm tra tài liệu hướng dẫn để xác định rằng nó có các chỉ dẫn để thiết lập hạn ngạch (nếu chúng có thể cấu hình được) và mô tả bất kỳ hành động nào người quản trị có thể hoặc nên thực hiện khi đạt đến một hạn ngạch.
Đánh giá	Đánh giá 1: Đánh giá viên thực hiện theo hướng dẫn hoạt động để định cấu hình hạn ngạch cho tài nguyên (nếu có khả năng đó). Đánh giá viên sau đó sẽ tạo ra việc vượt tới hạn ngạch và quan sát thấy rằng hành động được xác định trong TSS xảy ra.

B.1.5 IPS: Ngăn chặn xâm nhập

Trong trường hợp TOE hỗ trợ việc thực hiện chuẩn hóa các gói dữ liệu mạng, các yêu cầu sau đây có thể được bao gồm trong ST.

B.1.5.1 IPS_SBD_EXT.2 Chuẩn hóa lưu lượng mạng

IPS_SBD_EXT.2.1: TSF sẽ có thể kiểm tra các gói dữ liệu đóng gói thông qua các phương tiện sau đây:

- [lựa chọn: GRE, IP-in-IP, IPv4-in-IPv6, MPLS, PPTP, *[chỉ định: phương pháp đóng gói khác]*, không có các phương pháp khác]

Hoạt động	Hoạt động bảo đảm
TSS	Đánh giá viên phải xác minh rằng TSS mô tả TOE có thể kiểm tra lưu lượng trong các kênh truyền bên trong được xác định trong yêu cầu.
AGD	Đánh giá viên phải kiểm tra tài liệu hướng dẫn để xác định rằng nó có các chỉ dẫn để kiểm tra các gói tin thông qua các phương pháp đóng gói được xác định trong yêu cầu.
Đánh giá	Đánh giá 1: Đánh giá viên phải chạy lại bài kiểm tra dấu hiệu trước đó trong kênh truyền được xác định trong yêu cầu.

IPS_SBD_EXT.2.2: TSF sẽ có thể thực hiện chuẩn hóa IP để lắp ráp lại các gói tin bị phân mảnh để kiểm tra, và: [lựa chọn:

- Đối với dữ liệu thu thập tại các cổng promiscuous: tạo ra một cảnh báo nếu các gói tin không thể lắp ráp lại;

- Đối với dữ liệu thu thập tại các cổng nội tuyến: không gửi bất kỳ mảnh gói tin và tạo ra một cảnh báo nếu TSF không thể lắp ráp lại toàn bộ gói].

Hoạt động	Hoạt động bảo đảm
TSS	Đánh giá viên phải xác minh rằng TSS mô tả cách thức các bản ghi kiểm toán được tạo ra khi các gói không thể được lắp ráp lại sau khi phân mảnh. Ngoài ra, đối với chế độ nội tuyến, đánh giá viên phải kiểm tra TSS để đảm bảo các gói tin bị loại bỏ.
AGD	Không có hướng dẫn về hoạt động bảo đảm cho phần tử này.
Đánh giá	Đánh giá viên phải thực hiện các phép thử sau đây: Đánh giá 1: Đánh giá viên sẽ tạo ra các gói không thể lắp ráp sau khi phân mảnh; đánh giá viên phải đảm bảo các sự kiện kiểm toán được tạo ra cho tất cả các trường hợp chuẩn hóa IP. Đánh giá 2: Đối với chế độ nội tuyến: Đánh giá viên phải kiểm tra việc từ chối gói tin tự động khi các gói tin không thể được lắp ráp lại sau khi phân mảnh. Đánh giá viên phải chụp lại các gói tin để đảm bảo lưu lượng IP đã được TOE phát hiện và các gói dữ liệu bị loại bỏ. Đánh giá 3: Đánh giá viên sẽ tạo ra các gói có thể được lắp ráp sau khi phân mảnh; đánh giá viên phải đảm bảo các sự kiện kiểm toán được tạo ra cho tất cả các trường hợp chuẩn hóa IP.

IPS_SBD_EXT.2.3: TSF sẽ có thể thực hiện TCP bình thường cho lưu lượng chạy qua TOE khi TOE được triển khai trong chế độ nội tuyến, và cấm chuyển tiếp của: [lựa chọn:

- các gói trùng lặp;

- các gói bị thay đổi;

- các gói ngoài tuần tự;

- [lựa chọn: *[chỉ định: các loại gói khác mà không nên chuyển tiếp]*, không có gói khác]]

Hoạt động	Hoạt động đảm bảo
TSS	Đánh giá viên phải xác minh rằng TSS mô tả rằng các gói dữ liệu sẽ tự động bị loại bỏ trong các chuẩn hóa sau đây: - các gói trùng lặp - các gói bị thay đổi - các gói ngoài tuần tự - bất kỳ phương pháp khác được xác định trong yêu cầu.
AGD	Không có hướng dẫn về hoạt động đảm bảo cho phần tử này.

Đánh giá	Đánh giá 1: Đánh giá viên phải tạo ra các loại gói tin sau và quan sát thấy các gói dữ liệu bị loại bỏ: - Các gói trùng lặp - Các gói đã thay đổi - Các gói ngoài tuần tự - Bất kỳ phương pháp khác được xác định trong yêu cầu.

Phụ lục C

(Quy định)

Các yêu cầu dựa trên lựa chọn

Như đã nêu tại Phụ lục B của tiêu chuẩn này, các yêu cầu cơ bản (phải được đáp ứng bởi TOE hay trên nền tảng của TOE) được đưa ra trong phần nội dung của tiêu chuẩn này. Trường hợp đánh giá viên lựa chọn thêm yêu cầu dựa trên lựa chọn trong phần nội dung thì các yêu cầu dưới đây sẽ cần phải được đưa vào để đánh giá.

C.1 Yêu cầu

Các yêu cầu chức năng an toàn dựa trên lựa chọn được nêu trong các điều dưới đây.

C.1.1 FCS: Hỗ trợ mã hóa

Tiêu chuẩn này không đưa ra các yêu cầu lựa chọn mới liên quan đến hỗ trợ mã hóa, những yêu cầu này cũng chưa đưa ra trong NDPP hoặc FWPP. Tuy nhiên, trường hợp lựa chọn yêu cầu giao thức mạng an toàn trong FPT_ITT.1, thì đích đánh giá sẽ bao gồm các yêu cầu lựa chọn tương ứng trong NDPP hoặc FWPP đối với các giao thức mạng an toàn. Tác giả ST đánh giá các yêu cầu cần áp dụng trong TSF đối với các giao thức mạng an toàn trong PP cơ sở.

Phụ lục D

(Quy định)

Các yêu cầu mục tiêu

Như đã nêu tại Phụ lục B của tiêu chuẩn này, các yêu cầu cơ bản (phải được đáp ứng bởi TOE hoặc nền tảng của TOE) được đưa ra trong phần thân của tiêu chuẩn này. Những yêu cầu bổ sung về chức năng an toàn nêu trong Phụ lục này là khuyến khích sử dụng để đánh giá TOE và có thể sẽ được đưa vào yêu cầu cơ bản trong các phiên bản tiêu chuẩn tiếp theo.

D.1 Yêu cầu

Các yêu cầu chức năng an toàn mục tiêu được nêu trong các điều dưới đây.

D.1.1 FAU: Kiểm toán an toàn

Thuật ngữ "dữ liệu IPS" bao gồm tất cả các dữ liệu được trích xuất từ lưu lượng mạng và lưu trữ trên TOE; các kết quả phân tích được thực hiện bởi TOE; và các thông điệp thể hiện đáp ứng của TOE đối với các phân tích này. Định nghĩa này của "dữ liệu IPS" không bao gồm "dữ liệu kiểm toán" liên quan đến PP cơ sở, bao gồm dữ liệu định nghĩa tại FAU_GEN từ PP cơ sở, chẳng hạn như xác thực của các người quản trị, và thiết lập/chấm dứt kênh đáng tin cậy. Nếu TOE hỗ trợ soát xét và/hoặc lưu trữ dữ liệu IPS và các cảnh báo an toàn thì các yêu cầu đánh giá sau đây có thể được bao gồm trong ST.

D.1.1.1 FAU_ARP.1 Cảnh báo an toàn

FAU_ARP.1.1 TSF cần hỗ trợ *[chỉ định: danh sách các hành động]* khi phát hiện một vi phạm an toàn tiềm năng.

Chú thích áp dụng: Trong TCVN 8709-2, FAU_ARP được thiết kế phụ thuộc vào FAU_SAA để xác định một khả năng vi phạm các SFR. FAU_SAA không được bao gồm trong tiêu chuẩn này, và FRU_RSA được sử dụng thay thế để xác định "vi phạm an toàn tiềm năng" có liên quan đến FAU_ARP, cụ thể là TOE đã trải qua một sự tăng đột biến trong lưu lượng mạng đã vượt quá khả năng của nó để kiểm tra tất cả lưu lượng mạng, và sự kiện đó đã dẫn đến việc lưu lượng mạng bị rớt hoặc vượt qua mà không kiểm tra. SFR này nên được sử dụng để xác định hành động mà IPS TOE có thể thực hiện có thể bao gồm tạo ra một hoặc nhiều thông điệp không phải là một phần của dấu vết kiểm toán phải được truyền an toàn tới máy chủ kiểm toán từ xa. Tác vụ gửi thông điệp được định nghĩa bởi SFR này mà không liên quan cụ thể đến FAU_GEN.1/IPS không cần phải được mã hóa trong quá trình chuyển tiếp. Mục đích chính của chức năng này là đẩy nhanh thông báo, không phải là tính toàn vẹn hoặc tính bí mật của dữ liệu đang chuyển tiếp. Trong hầu hết các trường hợp, dấu vết kiểm toán áp dụng cho FAU_STG_EXT.1 sẽ là dữ liệu syslog và được bảo vệ khi chuyển tiếp để giúp đảm bảo tính toàn vẹn dữ liệu kiểm toán được lưu trữ từ xa. SFR này nhằm mục đích bao phủ truyền tải các thông báo liên quan đến các sự kiện đơn lẻ thông qua các giao thức như SNMP (trap) và SMTP (email). Trong các TOE hỗ trợ bảo vệ trap SNMP, email SMTP, hoặc các loại thông điệp khác trong các kênh đáng tin cậy (như định nghĩa bởi FTP_ITC.1), tác giả ST có thể chọn liệt kê các phương thức thông

báo này trong FTP_ITC.1 và/hoặc trong SFR này. Không có thêm sự kiện IPS có thể kiểm toán bổ sung cần phải được bao gồm trong FAU_GEN.1/IPS.

Hoạt động	Hoạt động bảo đảm
TSS	Đánh giá viên phải xác minh rằng TSS bao gồm một mô tả các cảnh báo được chỉ định trong yêu cầu. Đánh giá viên cũng phải xác minh rằng TSS cho biết dữ liệu kiểm toán không thể được truyền qua giao diện cảnh báo an toàn.
AGD	Đánh giá viên sẽ xác minh tài liệu hướng dẫn có giải thích làm thế nào để cho phép các cảnh báo được chỉ định trong yêu cầu như áp dụng cho FRU_RSA.1.
Đánh giá	Đánh giá 1: Đánh giá viên sẽ lập ra các bài kiểm tra chứng minh rằng việc truyền các thông điệp liên quan đến các sự kiện đơn lẻ thông qua các hành động được xác định. Lưu ý rằng hoạt động này có thể được giải quyết với sự kết hợp của các hoạt động đảm bảo kiểm tra cho IPS_ABD_EXT.1, IPS_SBD_EXT.1 và FRU_RSA.1.

D.1.1.2 FAU_SAR.1 Soát xét kiểm toán (dữ liệu IPS)

FAU_SAR.1.1 tinh chỉnh: TSF sẽ cung cấp [người quản trị có thẩm quyền] với khả năng đọc [*dữ liệu IPS*] từ các ~~bản kin kiểm toán~~ sự kiện IPS.

FAU_SAR.1.2 tinh chỉnh: TSF sẽ cung cấp ~~các bản tin kiểm toán~~ **dữ liệu IPS** một cách phù hợp tới ~~người dùng~~ **người quản trị** để giải thích các thông tin.

Chú thích áp dụng: Người ta dự kiến, nhưng không bắt buộc, TOE sẽ cung cấp một giao diện người dùng đồ họa mà cho phép tìm kiếm và phân loại, và sẽ chấp nhận những đầu ra gồm các nhóm sự kiện tương tự để dễ dàng soát xét quản trị dữ liệu IPS. Ví dụ, màn hình hiển thị có thể cho phép nhóm các dữ liệu theo loại sự kiện, hoặc theo địa chỉ IP nguồn, nơi nhiều sự kiện xảy ra trong một khoảng thời gian được hiển thị trên một dòng duy nhất như trong bảng mẫu dưới đây. Bất kể quan điểm như vậy được cung cấp hay không thì vẫn mong đợi những người quản trị sẽ có thể xem được chi tiết về sự xuất hiện của các sự kiện riêng rẽ. Không có thêm sự kiện IPS có thể kiểm toán bổ sung nào cần phải được đưa vào FAU_GEN.1 / IPS.

Bảng D-1: Bảng sự kiện (một số ví dụ đã được đưa vào)

Ngày/Giờ	Kiểu sự kiện	Phản ứng	Tổng số sự kiện
2013-01-1 10:45:00	Quét cổng từ IP 10.1.2.3	Chặn tất cả lưu lượng từ IP 10.1.2.3	34

Hoạt động	Hoạt động bảo đảm
TSS	Đánh giá viên sẽ kiểm tra để TSS xác minh rằng nó mô tả khả năng của người quản trị để xem dữ liệu IPS từ các sự kiện IPS, định dạng mà dữ liệu IPS này được hiển thị và cách người quản trị được ủy quyền để xem dữ liệu này.
AGD	Đánh giá viên sẽ kiểm tra tài liệu hướng dẫn để xác minh rằng nó cung cấp chỉ dẫn về cách truy cập và giải thích sự kiện IPS sử dụng giao diện quản lý của TOE.
Đánh giá	Đánh giá 1: Đánh giá viên sẽ lập ra những bài kiểm tra chứng minh rằng dữ liệu IPS (được tạo ra như đã định nghĩa trong FAU_GEN) có thể được giải thích bởi các người quản trị được ủy quyền từ giao diện quản lý của TOE.

D.1.1.3 FAU_SAR.2 Soát xét kiểm toán bị hạn chế (dữ liệu IPS)

FAU_SAR.2.1 tinh chỉnh: TSF sẽ cấm tất cả ~~người dùng~~ **người quản trị** đọc truy cập vào ~~các hồ sơ kiểm toán~~ **dữ liệu IPS,** ngoại trừ những người đã được gán rõ ràng quyền truy cập-đọc.

Chú thích áp dụng: Không có sự kiện IPS có thể kiểm toán bổ sung nào cần phải được đưa vào FAU_GEN.1/IPS.

Hoạt động bảo đảm
Vì vai trò quản trị là cần thiết để xem dữ liệu IPS, phân tích được thực hiện bởi các đánh giá viên trong hoạt động đảm bảo cho FMT_MTD.1/IPS sẽ chứng minh rằng yêu cầu này được đáp ứng.

D.1.1.4 FAU_SAR.3 Soát sét kiểm toán có thể lựa chọn (dữ liệu IPS)

FAU_SAR.3.1 tinh chỉnh: TSF sẽ cung cấp khả năng áp dụng [*lọc và sắp xếp*] dữ liệu ~~kiểm toán~~ **IPS** dựa trên [*thông số lọc: đánh giá rủi ro, khoảng thời gian, địa chỉ IP nguồn, địa chỉ IP đích và* [*lựa chọn: [chỉ định: thông số lọc khác]; không có thông số lọc khác]; và sắp xếp thông số: ID sự kiện, loại sự kiện, thời gian, ID chữ ký, hành động IPS thực hiện, và [lựa chọn: [chỉ định: thông số phân loại khác; không có thông số phân loại khác]]*.

Chú thích áp dụng: Không có sự kiện IPS có thể kiểm toán bổ sung nào cần phải được đưa vào FAU_GEN.1/IPS.

Hoạt động	Hoạt động bảo đảm
TSS	Đánh giá viên phải xác minh rằng TSS bao gồm mô tả TOE có khả năng áp dụng việc lọc và phân loại dữ liệu IPS sử dụng các tham số được liệt kê trong yêu cầu.
AGD	Đánh giá viên sẽ xem xét hướng dẫn quản trị để đảm bảo rằng các hướng dẫn sẽ phân loại các loại sự kiện, cũng như mô tả tất cả các thuộc tính được lựa chọn theo yêu cầu, bao gồm các thuộc tính được liệt kê trong chỉ định. Hướng dẫn quản trị cũng sẽ bao gồm các hướng dẫn về cách thiết lập lựa chọn trước, cũng như giải

	thích cú pháp (nếu có) cho các lựa chọn trước đa giá trị. Hướng dẫn quản trị cũng sẽ xác định những hồ sơ kiểm toán mà luôn được ghi lại, bất kể tiêu chí lựa chọn hiện đang được thi hành.
Đánh giá	Đánh giá viên phải thực hiện các phép thử sau đây: Đánh giá 1: Đối với mỗi thuộc tính được liệt kê trong yêu cầu, đánh giá viên sẽ lập ra một bài kiểm tra cho thấy rằng việc lựa chọn thuộc tính chỉ gây ra các sự kiện kiểm toán với thuộc tính đó (hoặc các thuộc tính luôn được ghi lại, như được xác định trong hướng dẫn quản trị) được ghi lại. Đánh giá 2 [có điều kiện]: Nếu TSF hỗ trợ đặc tả các tiêu chí lựa chọn trước phức tạp hơn (ví dụ, nhiều thuộc tính, các biểu thức lôgic sử dụng các thuộc tính) thì đánh giá viên phải đưa ra các kiểm tra cho thấy rằng khả năng này được thực hiện đúng. Đánh giá viên cũng phải, trong kế hoạch kiểm tra, cung cấp một bài tường thuật ngắn minh chứng cho bộ bài kiểm tra là đại diện và đủ để kiểm tra khả năng này.

Thư mục tài liệu tham khảo

[1] collaborative Protection Profile for Network Devices/ collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), Version 2.1 *(Hồ sơ bảo vệ cho thiết bị mạng/ Hồ sơ bảo vệ cho thiết bị tường lửa lọc lưu lượng có trạng thái – Gói mở rộng (EP) cho hệ thống phòng chống xâm nhập (IPS), Phiên bản 2.1*), NIAP, 15/6/2017.