TCVN

TIÊU CHUẨN QUỐC GIA

TCVN XXXXX:2026

Xuất bản lần 1

AN NINH MẠNG - SẢN PHẨM PHÒNG, CHỐNG XÂM NHẬP LỚP MẠNG - YÊU CẦU CHUNG

Cyber security - Network Intrusion Protection System - General requirements

HÀ NỘI – 2026

Mục lục

Lời nói đầu

TCVN XXXXX:2026 An ninh mạng - Sản phẩm phòng, chống xâm nhập lớp mạng - Yêu cầu chung do Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao biên soạn, Bộ Công an đề nghị, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Tiêu chuẩn này quy định các yêu cầu kỹ thuật đối với sản phẩm phòng, chống xâm nhập lớp mạng (NIPS), nhằm nâng cao năng lực giám sát, chia sẻ thông tin và chủ động bảo vệ hệ thống trước các mối đe dọa.

Để tối ưu hiệu quả cảnh báo sớm và ứng phó sự cố, các cơ quan, tổ chức được khuyến khích triển khai NIPS đáp ứng tiêu chuẩn này, kết hợp đồng bộ với các biện pháp quản lý, kỹ thuật và vận hành để xây dựng một hệ sinh thái phòng thủ toàn diện.

An ninh mạng - Sản phẩm phòng, chống xâm nhập lớp mạng - Yêu cầu chung

Cyber security - Network Intrusion Protection System - General requirements

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu kỹ thuật chung về an ninh mạng đối với sản phẩm phòng, chống xâm nhập lớp mạng (sau đây viết tắt là NIPS).

2 Tài liệu viện dẫn

Trong tiêu chuẩn này không có tài liệu nào được viện dẫn.

3 Thuật ngữ, định nghĩa và chữ viết tắt

Tiêu chuẩn này sử dụng các thuật ngữ, định nghĩa và chữ viết tắt dưới đây.

3.1 Thuật ngữ và định nghĩa

3.1.1

Phòng, chống xâm nhập lớp mạng (Network Intrusion Prevention System - NIPS)

Giải pháp chủ động giám sát lưu lượng truy cập, nhằm phát hiện và chặn đứng kịp thời các hành động tấn công, xâm nhập trái phép hoặc vô hiệu mã độc trước khi chúng gây hại cho hệ thống.

3.1.2

Hệ thống phát hiện và ngăn chặn xâm nhập mạng (Intrusion Detection and Prevention System - IDPS)

Hệ thống có toàn bộ các tính năng của IDS, đi kèm khả năng chủ động hành động để chặn đứng ngay lập tức các lưu lượng độc hại trước khi chúng xâm nhập vào hệ thống.

3.1.3

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

3.1.4

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.

3.1.5

Chế độ active - active (Active - Active)

Chế độ dự phòng độ sẵn sằng cao, trong đó các thiết bị đều ở trạng thái hoạt động, cùng tham gia xử lý lưu lượng và duy trì dịch vụ.

3.1.6

Chế độ actvie-standby (Active-Standby)

Chế độ dự phòng sẵn sàng cao, trong đó một thiết bị hoạt động chính và một hoặc nhiều thiết bị ở trạng thái dự phòng, thiết bị dự phòng tự động chuyển sang hoạt động khi thiết bị chính gặp sự cố.

3.1.7

Tầng ứng dụng (Application layer)

Tầng cao nhất trong các mô hình tham chiếu mạng (Tầng 7 trong mô hình OSI hoặc Tầng 4 trong mô hình TCP/IP). Đây là nơi cung cấp các giao diện, giao thức (như HTTP, FTP, DNS) để các ứng dụng phần mềm có thể giao tiếp, gửi và nhận dữ liệu qua mạng.

3.1.8

Chữ ký số (Digital Signature)

Một dạng chữ ký điện tử được tạo ra bằng thuật toán mã hóa khóa không đối xứng. Chữ ký số được gắn kèm với dữ liệu (văn bản, phần mềm) nhằm xác thực danh tính người ký, đảm bảo tính toàn vẹn của dữ liệu không bị thay đổi và chống chối bỏ trách nhiệm.

3.1.9

Chứng thư số (Digital Certificate)

Là một dạng chứng thư điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp nhằm cung cấp thông tin định danh cho khóa công khai của một cơ quan, tổ chức, cá nhân, từ đó xác nhận cơ quan, tổ chức, cá nhân là người ký chữ ký số bằng việc sử dụng khóa bí mật tương ứng.

3.1.10

Phân tích hồi tố (Retrospective Analysis)

Quá trình lưu trữ và liên tục phân tích lại các bản ghi mạng hoặc tệp tin đã quét trong quá khứ dựa trên các tri thức, bộ quy tắc về mối đe dọa (Threat Intelligence) mới nhất. Quá trình này giúp phát hiện ra các cuộc tấn công tinh vi đã từng lọt qua hệ thống phòng thủ vào thời điểm chưa có bản vá hoặc chưa nhận diện được.

3.1.11

Kiến trúc vi phân đoạn (Micro-segmentation)

Phương pháp thiết kế an ninh mạng chia trung tâm dữ liệu hoặc môi trường đám mây thành các phân vùng logic rất nhỏ (có thể cô lập đến từng máy ảo hoặc ứng dụng). Phương pháp này giúp áp dụng các chính sách bảo mật chi tiết, ngăn chặn tin tặc di chuyển ngang (lateral movement) trong trường hợp một phần hệ thống bị xâm nhập.

3.1.12

Container (Vùng chứa ứng dụng)

Một công nghệ ảo hóa cấp hệ điều hành, cho phép đóng gói mã nguồn phần mềm cùng tất cả các thư viện, môi trường phụ thuộc của nó thành một đơn vị tiêu chuẩn. Điều này giúp ứng dụng có thể chạy nhanh chóng, ổn định và nhất quán trên bất kỳ môi trường máy tính nào (ví dụ: Docker, Kubernetes).

3.1.13

Ảo hóa (Virtualization)

Công nghệ sử dụng phần mềm để tạo ra các phiên bản ảo của tài nguyên máy tính vật lý (bao gồm phần cứng, hệ điều hành, thiết bị lưu trữ, hoặc tài nguyên mạng). Công nghệ này giúp chạy nhiều hệ thống riêng biệt trên cùng một máy chủ vật lý, tối ưu hóa việc sử dụng tài nguyên.

3.1.14

Ngôn ngữ kịch bản (Scripting Engine)

Thành phần phần mềm hoặc môi trường thực thi cho phép hệ thống biên dịch và chạy các tập lệnh (scripts). Trong các hệ thống bảo mật, nó cho phép quản trị viên tùy chỉnh các quy tắc phân tích gói tin, tự động hóa phản hồi sự cố hoặc mở rộng tính năng của thiết bị.

3.1.15

Xác thực đa yếu tố (multi-factor authentication)

Phương pháp xác thực kết hợp một số yếu tố liên quan đến người dùng, bao gồm: những thông tin mà người dùng biết (mật khẩu, mã số truy cập...), những thông tin mà người dùng sở hữu (chứng thư chữ ký số, thẻ thông minh...), những thông tin về sinh trắc học của người dùng (vân tay, mống mắt...).

3.1.16

Danh sách trắng (whitelist)

Danh sách các thực thể riêng biệt đã được xác định, chấp thuận sử dụng trong hệ thống thông tin.

3.1.17

Danh sách đen (blacklist)

Danh sách các thực thể riêng biệt đã được xác định có liên quan đến hoạt động độc hại.

3.1.18

Chỉ báo xâm nhập (indicator of compromise - IoC)

Bằng chứng kỹ thuật hoặc dấu hiệu cho thấy một cuộc tấn công mạng sắp xảy ra, đang diễn ra hoặc có thể đã xảy ra.

3.1.19

Chế độ mở khi lỗi (Fail-Open)

Cơ chế cho phép lưu lượng đi qua khi xảy ra sự cố để duy trì dịch vụ

3.1.20

Cơ chế đóng khi có lỗi (fail-close)

Cơ chế không cho phép lưu lượng đi qua khi xảy ra sự cố.

3.1.21

Phân tích sâu gói tin (deep packet inspection)

Kỹ thuật kiểm tra và phân tích gói tin mạng, bao gồm tiêu đề và nội dung để phát hiện tấn công hoặc ứng dụng.

3.1.22

Thiết bị bảo mật phần cứng (hardware security module)

Là thiết bị hoặc hệ thống quản lý khóa mật mã chuyên dụng được tích hợp nhằm bảo vệ vòng đời khóa mã hóa và đảm bảo an toàn cho dữ liệu giải mã.

3.1.23

Đường cơ sở (baseline)

Là mức thông lượng và trạng thái lưu lượng mạng bình thường được xây dựng, định nghĩa và thiết lập nhằm phục vụ khả năng phát hiện các sự cố, hành vi bất thường của mạng.

3.2 Chữ viết tắt

IP	Giao thức Internet	Internet Protocol
MAC	Địa chỉ kiểm soát truy cập môi trường	Media Access Control
API	Giao diện lập trình ứng dụng	Application Programming Interface
CI/CD	Tích hợp và Triển khai liên tục	Continuous Integration / Continuous Deployment
DevSecOps	Bảo mật trong quy trình phát triển và vận hành	Development, Security, and Operations
VM	Máy ảo	Virtual Machine
IoC	Chỉ báo xâm nhập	Indicator of Compromise
MFA	Xác thực đa yếu tố	Multi-Factor Authentication
NIPS	Công cụ giám sát, phát hiện và phòng chống tấn công mức mạng	Network Intrusion Protection System
SIEM	Nền tảng quản lý, phân tích sự kiện và thông tin an ninh mạng	Security Information and Event Management
TI	Tình báo mối đe dọa	Threat Intelligence
SOAR	Điều phối, tự động hóa và phản hồi an ninh mạng	Security Orchestration, Automation and Response
IDS	Hệ thống phát hiện xâm nhập	Intrusion Detection System
IPS	Hệ thống phòng chống xâm nhập	Intrusion Prevention System
TLS	Giao thức bảo mật lớp truyền tải	Transport Layer Security
CPU	Bộ xử lý trung tâm	Central Processing Unit
RAM	Bộ nhớ truy cập ngẫu nhiên	Random Access Memory
Syslog	Giao thức ghi nhật ký hệ thống	System Logging Protocol

TCP	Giao thức điều khiển truyền dẫn	Transmission Control Protocol
UDP	Giao thức gói dữ liệu người dùng	User Datagram Protocol

4 Yêu cầu chung, quản trị và an toàn của nền tảng

4.1 Khái quát

Mục này quy định các yêu cầu về tài liệu, quản trị, vận hành và bảo đảm an toàn NIPS, nhằm bảo đảm hệ thống được triển khai, quản lý và duy trì an toàn, liên tục, tin cậy và có khả năng phục hồi khi xảy ra sự cố.

4.2 Yêu cầu cụ thể

4.2.1 Yêu cầu về tài liệu

4.2.1.1 Hướng dẫn triển khai và thiết lập cấu hình

NIPS phải được cung cấp kèm theo các tài liệu hướng dẫn sau:

a) Tài liệu hướng dẫn chi tiết các bước cài đặt, triển khai và thiết lập cấu hình NIPS.

b) Tài liệu hướng dẫn tinh chỉnh NIPS nhằm tối ưu hóa khả năng giám sát, giảm thiểu tỷ lệ cảnh báo sai và bỏ lọt tấn công; đồng thời cung cấp hướng dẫn thiết lập đường cơ sở phục vụ khả năng phát hiện sự cố bất thường.

4.2.1.2 Hướng dẫn sử dụng và quản trị

Tài liệu hướng dẫn chi tiết các chức năng sử dụng, phân quyền quản trị và quy trình vận hành NIPS.

4.2.2 Yêu cầu về quản trị hệ thống

4.2.2.1 Quản lý vận hành

NIPS cho phép quản lý, vận hành đáp ứng các yêu cầu sau:

a) Cho phép thiết lập danh sách trắng, danh sách đen dựa trên nhiều đối tượng mạng hơn, bao gồm: địa chỉ IP, dải IP, địa chỉ MAC và thông tin định vị địa lý;

b) Cho phép thay đổi thời gian hệ thống;

c) Cho phép thay đổi thời gian duy trì phiên kết nối;

d) Cho phép thiết lập, thay đổi các tham số giới hạn đối với kết nối quản trị từ xa (ví dụ: giới hạn địa chỉ IP, giới hạn số phiên kết nối quản trị từ xa đồng thời, ...);

đ) Cho phép đăng xuất tài khoản người dùng có phiên kết nối còn hiệu lực;

e) Cho phép tìm kiếm dữ liệu nhật ký bằng từ khóa để xem lại.

4.2.2.2 Quản trị từ xa

NIPS cho phép quản trị từ xa an toàn đáp ứng các yêu cầu sau:

a) NIPS có khả năng hỗ trợ và bắt buộc cấu hình xác thực đa yếu tố đối với mọi kết nối quản trị từ xa thông qua các giao thức an toàn;

b) Tự động đăng xuất tài khoản và hủy bỏ phiên kết nối quản trị từ xa khi hết thời gian duy trì phiên kết nối.

c) Cho phép cấu hình giới hạn IP quản trị, số lượng phiên đăng nhập và chống tấn công dò đoán mật khẩu.

4.2.2.3 Quản lý xác thực và phân quyền

NIPS cho phép quản lý cấu hình tài khoản xác thực và phân quyền người dùng đáp ứng các yêu cầu sau:

a) Hỗ trợ phương thức xác thực bằng tài khoản - mật khẩu, trong đó, quản trị viên có thể thiết lập và thay đổi được độ phức tạp của mật khẩu;

b) Hỗ trợ phân nhóm tài khoản tối thiểu theo 02 nhóm là quản trị viên và người dùng thường với những quyền hạn cụ thể đối với từng nhóm.

c) Đối với nhóm tài khoản có đặc quyền cao nhất, NIPS cung cấp tùy chọn bắt buộc kích hoạt xác thực đa yếu tố cho cả phiên đăng nhập cục bộ và từ xa.

d) Khi thay đổi quyền hạn tài khoản hoặc leo thang đặc quyền trong phiên kết nối, NIPS yêu cầu người dùng xác thực lại bằng yếu tố thứ hai.

đ) NIPS nên hỗ trợ xác thực tập trung thông qua các giao thức LDAP, Active Directory hoặc RADIUS.

4.2.3 Yêu cầu về kiểm soát lỗi

4.2.3.1 Bảo vệ cấu hình

Trong trường hợp NIPS phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), NIPS đảm bảo các loại cấu hình sau mà đang được áp dụng phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp:

a) Cấu hình NIPS;

b) Cấu hình quản trị từ xa;

c) Cấu hình tài khoản xác thực và phân quyền người dùng;

d) Cấu hình tập luật bảo vệ;

đ) Danh sách trắng địa chỉ IP;

e) Danh sách đen địa chỉ IP;

g) Danh sách các địa chỉ IP đang bị chặn kết nối.

4.2.3.2 Bảo vệ dữ liệu nhật ký, dữ liệu ứng dụng

Trong trường hợp NIPS phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), NIPS đảm bảo dữ liệu nhật ký đã được lưu lại phải không bị thay đổi trong lần khởi động kế tiếp.

4.2.3.3 Đồng bộ thời gian hệ thống

Trong trường hợp NIPS phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), NIPS đảm bảo thời gian hệ thống phải được đồng bộ tự động đến thời điểm hiện tại.

4.2.3.4 Sao lưu và phục hồi

NIPS phải có khả năng sao lưu và phục hồi các cấu hình và dữ liệu cần thiết để duy trì hoạt động của hệ thống, bao gồm tối thiểu:

a) Cấu hình NIPS;

b) Cấu hình quản trị từ xa;

c) Cấu hình tài khoản xác thực và phân quyền người dùng;

d) Cấu hình tập luật bảo vệ;

đ) Danh sách trắng địa chỉ IP;

e) Danh sách đen địa chỉ IP;

g) Danh sách các địa chỉ IP đang bị chặn kết nối.

Việc phục hồi phải bảo đảm các cấu hình và dữ liệu được áp dụng trước thời điểm xảy ra lỗi có thể được khôi phục phù hợp.

4.2.3.5 Cập nhật bản vá hệ thống

a) NIPS có chức năng cập nhật bản vá để xử lý các điểm yếu, lỗ hổng bảo mật của NIPS. Bản vá phải được kiểm tra chữ ký số của nhà sản xuất hoặc cơ chế xác thực toàn vẹn tương đương trước khi được áp dụng.

b) Hệ điều hành của NIPS phải được tinh gọn và thiết lập cấu hình an toàn, loại bỏ các dịch vụ và cổng kết nối không cần thiết dựa trên các khung tiêu chuẩn thực hành an toàn được công nhận.

c) NIPS có cơ chế khởi động an toàn nhằm ngăn chặn việc chèn mã độc vào tiến trình khởi động của thiết bị.

4.2.4 Yêu cầu về quản lý nhật ký

4.2.4.1 Nhật ký quản trị hệ thống

a) NIPS cho phép ghi nhật ký quản trị hệ thống về các loại sự kiện sau:

i) Đăng nhập, đăng xuất tài khoản;

ii) Xác thực trước khi cho phép truy cập vào tài nguyên, sử dụng chức năng của hệ thống;

iii) Áp dụng, hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình tập luật bảo vệ;

iv) Kích hoạt lệnh khởi động lại, tắt hệ thống;

v) Thay đổi thủ công thời gian hệ thống;

vi) Có sự thay đổi trạng thái liên kết của giao diện giám sát.

b) NIPS cho phép ghi nhật ký quản trị hệ thống có các trường thông tin sau:

i) Thời gian sinh nhật ký (bao gồm năm, tháng, ngày, giờ, phút và giây);

ii) Địa chỉ IP hoặc định danh của máy trạm;

iii) Định danh của tác nhân (ví dụ: tài khoản người dùng, tên hệ thống, ...);

iv) Thông tin về hành vi thực hiện (ví dụ: đăng nhập, đăng xuất, thêm, sửa, xóa, cập nhật, hoàn tác, ...);

v) Kết quả thực hiện hành vi (thành công hoặc thất bại);

vi) Lý do giải trình đối với hành vi thất bại (ví dụ: không tìm thấy tài nguyên, không đủ quyền truy cập, ...);

vii) Phân loại theo mức độ rủi ro hoặc mức độ nghiêm trọng của sự kiện quản trị.

4.2.4.2 Nhật ký cảnh báo

4.2.4.2.1 Nhật ký chức năng phát hiện và ngăn chặn xâm nhập mạng

a) NIPS cho phép ghi nhật ký tất cả các sự kiện về hành vi xâm nhập mạng phát hiện được.

b) NIPS cho phép ghi nhật ký chức năng phát hiện và ngăn chặn xâm nhập mạng có các trường thông tin sau:

i) Thời gian sinh nhật ký (bao gồm năm, tháng, ngày, giờ, phút và giây);

ii) Địa chỉ IP của máy nguồn, địa chỉ IP của máy đích;

iii) Số hiệu cổng nguồn, số hiệu cổng đích;

iv) Tên giao thức;

v) Mô tả của hành vi xâm nhập mạng phát hiện được, mức độ nghiêm trọng, kết quả hành động, mã sự kiện nếu có;

vi) Giao diện mạng vật lý hoặc ảo hóa nơi gói tin bị vi phạm được tiếp nhận;

vii) Cấu trúc dữ liệu, trường tiêu đề hoặc chuỗi văn bản cụ thể của gói tin đã làm kích hoạt luật bảo vệ hệ thống.

viii) Nhật ký phát hiện tấn công phải bao gồm hoặc hỗ trợ ánh xạ tới các khung tiêu chuẩn phân loại kỹ thuật và chiến thuật tấn công mạng quốc tế để phân loại rõ ngữ cảnh rủi ro.

ix) NIPS có khả năng tự động lưu trữ và cho phép tải về gói tin thô của luồng giao tiếp trước và sau khi phát sinh cảnh báo rủi ro cao.

4.2.4.2.2 Định dạng nhật ký

NIPS cho phép chuẩn hóa nhật ký theo tối thiểu 01 định dạng được định nghĩa trước để truyền dữ liệu nhật ký cho các phần mềm quản lý, phân tích, điều tra.

4.2.4.3 Quản lý vòng đời lưu trữ nhật ký

NIPS cho phép quản lý vòng đời nhật ký đáp ứng các yêu cầu sau:

a) Cho phép thiết lập và cấu hình các cài đặt liên quan đến lưu trữ và hủy bỏ nhật ký (ví dụ: ngưỡng giới hạn dung lượng lưu trữ, khoảng thời gian lưu trữ...).

b) Cho phép tìm kiếm nhật ký theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có);

c) Cho phép xuất dữ liệu nhật ký ra để phục vụ cho việc tích hợp các dữ liệu này vào SIEM hoặc giải pháp khác về quản lý, phân tích, điều tra.

5 Yêu cầu về chức năng nghiệp vụ của nền tảng

5.1 Khái quát

Mục này quy định các yêu cầu về chức năng nghiệp vụ của NIPS, bao gồm khả năng thu thập, phân tích và xử lý dữ liệu lưu lượng mạng; quản lý chỉ báo, luật và tri thức mối đe dọa; phát hiện, cảnh báo và ngăn chặn xâm nhập; chia sẻ, tích hợp dữ liệu; lập báo cáo; đồng thời bảo đảm hiệu năng, khả năng mở rộng, dự phòng và phục hồi của hệ thống.

5.2 Yêu cầu cụ thể

5.2.1 Thu thập, tiếp nhận và mô hình hóa dữ liệu tình báo

Đối với NIPS, nhóm yêu cầu này tập trung vào khả năng tiếp nhận, nhận diện và mô hình hóa thông tin phục vụ phân tích lưu lượng và tình báo mối đe dọa.

5.2.1.1 Quản lý các giao diện mạng

NIPS cho phép quản lý cấu hình NIPS về các giao diện mạng đáp ứng các yêu cầu sau:

a) Cho phép thiết lập một hoặc một số giao diện giám sát ở chế độ giám sát chủ động hoặc chế độ giám sát thụ động hoặc kết hợp cả hai chế độ;

b) Cho phép thiết lập tối thiểu một giao diện quản trị, khác với giao diện giám sát, để thực hiện:

i) Quản trị hệ thống;

ii) Tương tác với các thiết bị mạng khác nếu có.

5.2.1.2 Hỗ trợ các giao thức mạng

NIPS cho phép phân tích thông tin trên lưu lượng mạng được giám sát đối với các giao thức mạng sau:

a) Giao thức IPv4 (RFC 791);

b) Giao thức IPv6 (RFC 8200);

c) Giao thức ICMPv4 (RFC 792);

d) Giao thức ICMPv6 (RFC 4443);

đ) Giao thức TCP (RFC 9293);

e) Giao thức UDP (RFC 768);

g) Giao thức mạng: SMB, DCERPC, DNS, HTTP.

h) Hỗ trợ nhận diện và phân tích tối thiểu đối với các giao thức công nghiệp phổ biến: Modbus TCP, DNP3, IEC 60870-5-104, MQTT.

5.2.1.3 Khả năng nhận diện ứng dụng

a) NIPS có khả năng nhận diện, phân tích và áp dụng các luật kiểm soát đối với lưu lượng mạng dựa trên đặc điểm kỹ thuật và bản chất của ứng dụng tại Tầng ứng dụng (Lớp 7 theo mô hình OSI).

b) Quá trình nhận diện phải được thực hiện thông qua các kỹ thuật kiểm tra sâu, như thuật toán phân tích hành vi suy luận, đối sánh mẫu, bảo đảm tính độc lập và chính xác kể cả trong trường hợp ứng dụng sử dụng cổng giao thức TCP/UDP phi tiêu chuẩn, cổng chia sẻ hoặc thay đổi cổng động.

5.2.1.4 Khả năng nhận thức ngữ cảnh

NIPS cho phép tích hợp và liên kết các thông tin ngữ cảnh đa chiều vào tập luật bảo vệ và quá trình phân tích sự kiện mạng. Các thông tin ngữ cảnh được hỗ trợ tối thiểu bao gồm:

a) Định danh và vai trò của người dùng gắn với phiên kết nối;

b) Đặc điểm nhận dạng của thiết bị đầu cuối;

c) Tình trạng thiết bị;

d) Thông tin định vị địa lý.

5.2.2 Xử lý dữ liệu tình báo

5.2.2.1 Phân tích thông tin trong phần tiêu đề gói tin

NIPS cho phép phân tích các trường thông tin sau trong phần tiêu đề của các gói tin thuộc lưu lượng mạng được giám sát:

a) Đối với giao thức IPv4: Version, Header Length, Packet Length, ID, Flags, Fragment Offset, Time to Live, Protocol, Header Checksum, Source Address, Destination Address, Options;

b) Đối với giao thức IPv6: Version, Payload Length, Next Header, Hop Limit, Source Address, Destination Address, Routing Header;

c) Đối với giao thức ICMPv4 và ICMPv6: Type, Code, Header Checksum;

d) Đối với giao thức TCP: Source Port, Destination Port, Sequence Number, Acknowledgment Number, Data Offset, Reserved, Flags, Window, Packet Checksum, Urgent Pointer, Options;

đ) Đối với giao thức UDP: Source Port, Destination Port, Payload Length, Packet Checksum.

5.2.2.2 Phân tích thông tin trong phần dữ liệu gói tin

NIPS cho phép phân tích các trường thông tin sau trong phần dữ liệu của các gói tin thuộc lưu lượng mạng được giám sát:

a) Đối với giao thức ICMPv4 và ICMPv6: chuỗi dữ liệu sau 4 byte đầu tiên của phần tiêu đề;

b) Đối với giao thức TCP: chuỗi dữ liệu sau 20 byte của phần tiêu đề, kiểm tra với các thông tin sau:

i) Đối với giao thức FTP: help, noop, stat, syst, user, abort, acct, alio, appe, cdup, cwd, dele, list, mkd, mode, nist, pass, pasv, port, pass, quit, rein, rest, retr, rmd, rnfr, rnto, site, smnt, stor, stou, stru và type;

ii) Đối với giao thức HTTP: phương thức GET, phương thức POST, so khớp nội dung trên URL/URI và nội dung trang web;

iii) Đối với giao thức SMTP: start State, commands State, mail header State, mail body State, abort State.

c) NIPS có khả năng duy trì bảng máy trạng thái cho các giao thức ứng dụng. Hệ thống có khả năng nhận diện và ngăn chặn các giao tiếp vi phạm trình tự hợp lệ của ngữ cảnh giao thức;

d) NIPS cung cấp ngôn ngữ kịch bản cho phép tự định nghĩa bộ bóc tách để kiểm tra sâu dữ liệu của các giao thức hoặc ứng dụng đặc thù.

5.2.2.3 Tấn công trên phần dữ liệu

NIPS cho phép phát hiện hành vi xâm nhập mạng dựa trên phân tích dấu hiệu đối với các phần dữ liệu của nhiều gói tin không bị phân mảnh.

5.2.2.4 Chuẩn hóa, tái lắp ghép và chống lẩn tránh

NIPS phải hỗ trợ các kỹ thuật xử lý dữ liệu và chống kỹ thuật lẩn tránh sau:

a) Tái tổ hợp các phân mảnh IP;

b) Tái tổ hợp luồng TCP, xử lý các gói tin lỗi tuần tự và loại bỏ các gói TCP trùng lặp/giả mạo;

c) Giải mã trước khi xử lý các phần dữ liệu tải bị xáo trộn mã hóa trước khi quét tìm chữ ký;

d) NIPS có khả năng hỗ trợ tính năng giải mã nội tuyến để kiểm tra sâu gói tin đối với các luồng giao tiếp mã hóa mà không làm suy giảm nghiêm trọng băng thông của hệ thống;

đ) NIPS có khả năng tích hợp với các hệ thống quản lý khóa mật mã chuyên dụng hoặc thiết bị bảo mật phần cứng để bảo vệ vòng đời khóa mã hóa;

e) NIPS có cơ chế hủy khóa an toàn khi thay đổi cấu hình hoặc gỡ bỏ chứng thư số, bảo đảm dữ liệu giải mã trong quá khứ không thể bị khôi phục trái phép;

g) NIPS có khả năng trích xuất và phân tích các siêu dữ liệu của luồng kết nối mã hóa, ví dụ: thông tin chứng thư số, chuẩn mã hóa, băm dấu vân tay máy khách/máy chủ, để phát hiện lưu lượng sinh ra từ mã độc hoặc các công cụ lẩn tránh mà không yêu cầu giải mã hoàn toàn dữ liệu tải.

5.2.3 Quản lý vòng đời chỉ báo và tri thức mối đe dọa

5.2.3.1 Quản lý tập luật bảo vệ

NIPS cho phép quản lý tập luật bảo vệ bao gồm các thao tác sau:

a) Thêm luật mới;

b) Tinh chỉnh luật;

c) Tìm kiếm luật;

d) Xóa luật;

đ) Kích hoạt/vô hiệu hóa luật;

e) Xuất tập luật ra tệp tin;

g) Khôi phục tập luật từ tệp tin.

5.2.3.2 Cập nhật tập luật bảo vệ

NIPS cho phép cập nhật tập luật bảo vệ đáp ứng các yêu cầu sau:

a) Cho phép tự động thông báo có bản cập nhật mới cho quản trị viên;

b) Cho phép tải về trực tuyến và áp dụng thủ công bản cập nhật mới;

c) Cập nhật tập luật được phát hành bởi nhà sản xuất. Yêu cầu kiểm tra chữ ký số tệp tải về hoặc cơ chế xác thực tương đương; hỗ trợ khôi phục tập luật khi cập nhật lỗi.

5.2.3.3 Quản lý danh sách trắng và danh sách đen địa chỉ IP

NIPS cho phép thực hiện các thao tác sau để quản lý các danh sách trắng địa chỉ IP và danh sách đen địa chỉ IP:

a) Thêm, xóa, sửa địa chỉ/dải địa chỉ IP;

b) Tìm kiếm theo địa chỉ/dải địa chỉ IP;

c) Thiết lập hành động kiểm soát lưu lượng mạng với địa chỉ/dải địa chỉ IP;

d) Kích hoạt/vô hiệu hóa hành động kiểm soát lưu lượng mạng đang được áp dụng đối với địa chỉ/dải địa chỉ IP;

đ) Xuất danh sách địa chỉ/dải địa chỉ IP ra tệp tin;

e) Khôi phục danh sách địa chỉ/dải địa chỉ IP từ tệp tin;

g) Đối với danh sách trắng, cho phép thiết lập, thay đổi thời hạn hiệu lực.

5.2.3.4 Quản lý tập các địa chỉ IP đang bị chặn kết nối

NIPS cho phép thực hiện các thao tác sau để quản lý tập các địa chỉ IP đang bị chặn kết nối:

a) Tìm kiếm các địa chỉ IP đang bị chặn kết nối theo địa chỉ IP, từ khóa;

b) Xem các thông tin về một địa chỉ IP đang bị chặn kết nối, tối thiểu bao gồm: thời điểm bắt đầu chặn kết nối, khoảng thời gian chặn kết nối có hiệu lực tính từ thời điểm bắt đầu, số hiệu định danh của luật gây ra việc chặn kết nối;

c) Hủy chặn kết nối đối với một hoặc nhiều địa chỉ IP cùng lúc đang bị chặn kết nối.

5.2.3.5 Tích hợp thông tin tình báo mối đe dọa

NIPS cho phép tích hợp và quản lý dữ liệu tình báo mối đe dọa đáp ứng các yêu cầu sau:

a) Có khả năng tiếp nhận và tự động cập nhật các chỉ báo xâm nhập từ các nguồn tình báo bên ngoài mà không cần cập nhật toàn bộ tập luật;

b) Hỗ trợ tiếp nhận luồng dữ liệu tình báo theo các định dạng tiêu chuẩn quốc tế hoặc tiêu chuẩn tương đương.

5.2.3.6 Phát hiện tấn công dựa trên chữ ký

a) NIPS có khả năng phát hiện và ngăn chặn các hành vi xâm nhập mạng thông qua việc đối sánh lưu lượng với cơ sở dữ liệu các chữ ký tấn công đã biết;

b) NIPS cho phép quản trị viên tùy biến và gán các tập chữ ký khác nhau cho từng giao diện mạng, phân đoạn mạng hoặc chiều lưu lượng cụ thể nhằm kiểm soát chính xác các đối tượng mạng;

c) NIPS có khả năng hỗ trợ các định dạng chữ ký tiêu chuẩn phổ biến để cho phép tùy biến và định nghĩa luật bảo vệ thủ công.

5.2.3.7 Phát hiện dựa trên sự bất thường

a) NIPS có khả năng hỗ trợ xây dựng và định nghĩa đường cơ sở lưu lượng mạng;

b) NIPS có khả năng tự động sinh cảnh báo và kích hoạt hành động ngăn chặn đối với các sự cố bất thường dựa trên: giới hạn thông lượng, tần suất sự kiện và thời điểm bất thường trong ngày;

c) NIPS có khả năng ứng dụng các thuật toán học máy để phân tích đặc điểm nhận dạng và phát hiện các hành vi liên lạc bất thường, điển hình như: thuật toán sinh tên miền tự động, liên lạc với máy chủ điều khiển hoặc kỹ thuật truyền dữ liệu nhỏ giọt;

d) NIPS có khả năng phân tích hồi tố, cho phép tự động đối chiếu các dấu hiệu thỏa hiệp và tập luật mới cập nhật với kho dữ liệu nhật ký và siêu dữ liệu mạng trong quá khứ.

5.2.3.8 Hỗ trợ quản lý tài sản và lỗ hổng

NIPS có khả năng tích hợp thông tin tài sản, cấu hình và lỗ hổng bảo mật để phục vụ phân tích ngữ cảnh sự cố.

5.2.4 Chia sẻ, phân phối, tích hợp và kiểm soát sử dụng dữ liệu

5.2.4.1 Chia sẻ dữ liệu

a) NIPS hỗ trợ tối thiểu một định dạng chuẩn như Syslog, CEF, LEEF hoặc JSON;

b) Truyền nhật ký qua kênh an toàn có mã hóa như TLS hoặc tương đương.

5.2.4.2 Tích hợp với hệ thống SIEM và các hệ thống giám sát, phân tích, điều tra khác

a) NIPS cho phép kết nối với các loại hệ thống SIEM để chia sẻ dữ liệu;

b) NIPS có khả năng phân định rõ ràng và cung cấp cấu hình luồng dữ liệu độc lập giữa "Nhật ký hệ thống/quản trị" và "Nhật ký phát hiện xâm nhập" khi tiến hành chia sẻ và tích hợp dữ liệu với các hệ thống SIEM bên ngoài.

c) NIPS cho phép kết nối với các hệ thống giám sát, phân tích và điều tra an ninh mạng khác thông qua các định dạng dữ liệu tiêu chuẩn được hỗ trợ.

5.2.4.3 Tích hợp nền tảng điều phối, tự động hóa và phản ứng an ninh mạng

NIPS cung cấp API mở, cho phép các hệ thống SOAR tương tác hai chiều để tự động hóa quá trình truy vấn thông tin, điều tra sự cố và thực thi các hành động ngăn chặn.

5.2.4.4 API và tự động hóa

a) NIPS cung cấp API an toàn để hỗ trợ tự động hóa việc cấu hình, cập nhật tập luật bảo vệ và tích hợp với các đường ống triển khai liên tục (CI/CD);

b) Việc tích hợp API phải hỗ trợ các cơ chế xác thực, phân quyền và bảo vệ kênh truyền nhằm bảo đảm an toàn trong quá trình phát triển, triển khai và cập nhật sản phẩm.

5.2.4.5 Tích hợp môi trường điện toán đám mây

a) NIPS hỗ trợ triển khai linh hoạt dưới dạng máy ảo hoặc kiến trúc vùng chứa;

b) NIPS có khả năng tự động áp dụng các đường cơ sở bảo mật khi hạ tầng điện toán đám mây mở rộng hoặc thu hẹp quy mô;

c) NIPS có khả năng giám sát và bảo vệ lưu lượng mạng nội bộ thông qua việc triển khai các cảm biến phân tán hoặc tích hợp với kiến trúc vi phân đoạn.

5.2.5 Thống kê xu hướng, cảnh báo và báo cáo

5.2.5.1 Quản lý báo cáo

NIPS cho phép quản lý báo cáo thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo;

b) Cho phép tạo báo cáo mới theo các mẫu báo cáo đã được định nghĩa trước;

c) Cho phép áp dụng các quy tắc tìm kiếm thông tin, dữ liệu log để thêm, lọc, tinh chỉnh nội dung cho báo cáo;

d) Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 02 trong các định dạng sau: WORD, EXCEL, PDF, HTML, XML;

đ) Cho phép tải về tệp tin báo cáo đã được xuất ra.

5.2.5.2 Cơ chế thực thi bảo vệ

NIPS đảm bảo thực hiện quá trình phân tích thông tin trên lưu lượng mạng được giám sát theo đúng thứ tự ưu tiên xử lý của các tập luật bảo vệ, danh sách trắng địa chỉ IP, danh sách đen địa chỉ IP đã được cấu hình, trong đó tối thiểu một thứ tự đã được cấu hình mặc định trước bởi nhà sản xuất.

5.2.5.3 Phát hiện các dạng tấn công

Xét trong môi trường kiểm thử, NIPS có khả năng phát hiện tối thiểu các dạng tấn công lớp mạng phổ biến sau:

a) Tấn công IP Fragments Overlap, ví dụ: Teardrop, Bonk/Boink;

b) Tấn công có địa chỉ IP nguồn và đích trùng nhau, ví dụ: Land;

c) Tấn công Fragmented ICMP Traffic, ví dụ: Nuke;

d) Tấn công Large ICMP Traffic, ví dụ: Ping of Death;

đ) Tấn công TCP NULL flags;

e) Tấn công TCP SYN+FIN flags;

g) Tấn công TCP FIN flags;

h) Tấn công TCP SYN+RST flags;

i) Tấn công UDP Bomb;

k) Tấn công UDP Chargen DoS;

l) Tấn công Flooding a host, ví dụ: Smurf, Ping Flood, SYN Flood;

m) Tấn công Flooding a network;

n) Tấn công IP protocol scanning;

o) Tấn công TCP port scanning;

p) Tấn công UDP port scanning;

q) Tấn công ICMP scanning.

5.2.5.4 Cảnh báo và kiểm soát lưu lượng mạng

5.2.5.4.1 Cảnh báo

NIPS có khả năng sinh cảnh báo đối với các sự kiện phát hiện, ngăn chặn xâm nhập mạng và các sự cố bất thường.

5.2.5.4.2 Kiểm soát lưu lượng mạng

a) NIPS cho phép thiết lập hành động kiểm soát lưu lượng mạng và khoảng thời gian hiệu lực của hành động đó, nếu có thể, đối với từng luật bảo vệ tối thiểu thuộc 01 trong các hành động sau:

i) Cho phép tiếp tục kết nối;

ii) Gửi gói tin TCP RST về phía địa chỉ nguồn;

iii) Gửi gói tin TCP RST về phía địa chỉ đích;

iv) Gửi gói tin phản hồi ICMP Destination Unreachable.

v) Loại bỏ gói tin, không phản hồi.

Các hành động tại ii) và iii) chỉ áp dụng đối với luật bảo vệ tương ứng với lưu lượng giao thức TCP.

b) Trong trường hợp NIPS vận hành theo chế độ giám sát chủ động, NIPS cho phép thiết lập hành động chặn kết nối đối với từng luật bảo vệ đáp ứng các yêu cầu sau:

i) Cho phép chặn kết nối theo địa chỉ IP nguồn phát sinh sự kiện;

ii) Cho phép chặn kết nối theo địa chỉ IP đích phát sinh sự kiện.

5.2.6 Hiệu năng xử lý, khả năng mở rộng và phục hồi

5.2.6.1 Yêu cầu về hiệu năng xử lý

NIPS phải được triển khai theo đúng cấu hình phần cứng tối thiểu đã được nhà sản xuất công bố tại tài liệu hướng dẫn cài đặt và thiết lập cấu hình (xem 4.2.1.1).

Nhà sản xuất phải công bố các thông số hiệu năng tối thiểu tương ứng với cấu hình phần cứng tối thiểu nêu trên, bao gồm tối thiểu:

a) Số lượng kết nối trên giây;

b) Số lượng kết nối đồng thời tối đa.

Việc đánh giá hiệu năng băng thông và độ trễ phải được tiến hành bằng các bài kiểm tra áp dụng lưu lượng hỗn hợp ở Lớp 7 (Application Layer) như HTTP/HTTPS. NIPS được coi là đáp ứng yêu cầu tại điều này nếu kết quả đo được không thấp hơn các thông số đã công bố tại điểm a), b) nêu trên.

5.2.6.2 Khả năng chịu lỗi vận hành

a) Trong trường hợp NIPS gặp lỗi trong quá trình vận hành ở chế độ giám sát chủ động, NIPS phải cho phép tự động kích hoạt chức năng bỏ qua kiểm soát và cho phép quản trị viên kích hoạt thủ công chức năng này. Khi kích hoạt phải sinh cảnh báo và ghi nhật ký;

b) Có khả năng cấu hình fail-open hoặc fail-close;

c) Khi vận hành ở chế độ fail-close, NIPS có cơ chế ngăn chặn hoàn toàn lưu lượng đi qua giao diện nội tuyến nếu chức năng kiểm tra sâu bị gián đoạn. NIPS bắt buộc phải sinh cảnh báo khi tài nguyên phần cứng, gồm CPU, RAM, phiên kết nối, đạt tới hạn mức tối đa.

5.2.6.3 Dự phòng và tính sẵn sàng

a) NIPS hỗ trợ triển khai theo kiến trúc dự phòng cụm ở tối thiểu một trong hai chế độ: Active-Active hoặc Active-Passive;

b) Trong quá trình chuyển đổi dự phòng khi có sự cố, hệ thống phải có cơ chế đồng bộ trạng thái để bảo đảm các phiên kết nối mạng đang hợp lệ không bị gián đoạn.

5.2.6.4 Cơ chế vá lỗi ảo

a) NIPS cung cấp cơ chế vá lỗi ảo, cho phép áp dụng các luật bảo vệ được ánh xạ trực tiếp tới các mã lỗ hổng bảo mật phổ biến;

b) NIPS có khả năng đề xuất hoặc tự động kích hoạt các luật vá lỗi ảo tương ứng dựa trên cấu hình hệ điều hành và ứng dụng mục tiêu đang được bảo vệ.

Tài liệu tham khảo

[1] TCVN 14423:2026 An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản.

[2] Tiêu chuẩn: TCVN 12820:2020 - Công nghệ thông tin - Các kỹ thuật an toàn.

[3] IDS/IPS Security Requirements Guide (SRG).

[4] NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems – IDPS.

[5] NetSecOPEN RFC 9411

[6] INTERNATIONAL STANDARD ISO/IEC 27039

[7] RFC 6274 - Security Assessment of the Internet Protocol Version 4 - IETF Datatracker

[8] Intrusion Detection and Prevention Systems - National Institute of Standards and Technology.

[9] Intrusion Detection, Evasion, and Trace Analysis - GIAC Certifications.

[10] Quyết định số 1591/QĐ-BTTTT yêu cầu kỹ thuật cơ bản đối với sản phẩm phòng, chống xâm nhập lớp mạng.

[11] NIAP PP-Module for IPS Version 2.0: Mô-đun Hồ sơ Bảo vệ cho IPS Phiên bản 2.0 của Hiệp hội Đảm bảo Thông tin Quốc gia Hoa Kỳ.