

**THUYẾT MINH DỰ THẢO TIÊU CHUẨN QUỐC GIA**  
**AN NINH MẠNG - SẢN PHẨM PHÒNG, CHỐNG XÂM NHẬP LỚP**  
**MẠNG - YÊU CẦU CHUNG**

**1. Thông tin chung về dự thảo TCVN**

a) Tên dự thảo TCVN

TCVN XXXXX:2026, An ninh mạng - Sản phẩm phòng, chống xâm nhập lớp mạng - Yêu cầu chung.

b) Thuộc lĩnh vực

Tiêu chuẩn thuộc lĩnh vực tiêu chuẩn cho sản phẩm, dịch vụ an ninh mạng.

c) Phạm vi áp dụng của TCVN

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).

d) Mục tiêu của TCVN

Tạo lập một hệ quy chiếu đo lường và kiểm định kỹ thuật thống nhất, làm căn cứ pháp lý độc lập cho công tác đánh giá, cấp chứng nhận hợp chuẩn sản phẩm trước khi đưa vào lưu hành. Tiêu chuẩn sẽ đóng vai trò là thước đo kỹ thuật bắt buộc để các cơ quan nhà nước và chủ quản hệ thống thông tin trọng yếu tham chiếu trong quá trình thiết kế kiến trúc, lập hồ sơ thầu và nghiệm thu. Đồng thời, đây cũng là định hướng cho các doanh nghiệp công nghệ trong nước chuẩn hóa kiến trúc phần cứng và tối ưu hóa bộ luật nhận diện, tạo đòn bẩy thúc đẩy quá trình nghiên cứu, phát triển sản phẩm NIPS "Make in Vietnam" đạt chất lượng tương đương quốc tế và đáp ứng toàn diện yêu cầu bảo vệ chủ quyền trên không gian mạng.

đ) Cơ quan chủ trì soạn thảo

- Tên cơ quan: Cục An ninh mạng và phòng, chống tội phạm sử dụng Công nghệ cao
- Bộ Công an.
- Địa chỉ: Lô E2, khu đô thị mới Cầu Giấy, Phường Cầu Giấy, Thành phố Hà Nội.

e) Tổ chức tham gia soạn thảo

Tham gia soạn thảo tiêu chuẩn quốc gia (TCVN) này bao gồm: Các cán bộ Trung tâm An ninh mạng quốc gia thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng Công nghệ cao; Các chuyên gia của Hiệp hội An ninh mạng quốc gia; Công ty Cổ phần Công nghệ An ninh mạng Quốc gia Việt Nam (NCS Group).

g) Phiên bản dự thảo: Version 1

**2. Nội dung dự thảo TCVN**

| <b>DỰ THẢO TCVN</b>                                       | <b>THUYẾT MINH</b>                                                                                                                                                          |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1. Phạm vi áp dụng</b>                                 | Tự xây dựng.                                                                                                                                                                |
| <b>2. Tài liệu viện dẫn</b>                               | Tự xây dựng.                                                                                                                                                                |
| <b>3. Thuật ngữ, định nghĩa và chữ viết tắt</b>           | Tham khảo Mục I.3. Khái niệm và thuật ngữ của Quyết định số 1591/QĐ-BTTTT. Bổ sung các khái niệm về chế độ hoạt động (Promiscuous, Inline) dựa trên NIAP PP-Module for IPS. |
| <b>4. Yêu cầu chung, quản trị và an toàn của nền tảng</b> | Tự xây dựng.                                                                                                                                                                |
| 4.1 Khái quát                                             | Tự xây dựng.                                                                                                                                                                |
| 4.2 Yêu cầu cụ thể                                        | Tự xây dựng.                                                                                                                                                                |
| 4.2.1 Yêu cầu về tài liệu                                 | Tham khảo Mục II.1. Yêu cầu về tài liệu của Quyết định số 1591/QĐ-BTTTT.                                                                                                    |
| 4.2.1.1 Hướng dẫn triển khai và thiết lập cấu hình        | Tham khảo Mục II.1. Yêu cầu về tài liệu của Quyết định số 1591/QĐ-BTTTT.                                                                                                    |
| 4.2.1.2 Hướng dẫn sử dụng và quản trị                     | Tham khảo Mục II.1. Yêu cầu về tài liệu của Quyết định số 1591/QĐ-BTTTT.                                                                                                    |
| 4.2.2 Yêu cầu về quản trị hệ thống                        | Tham khảo Mục II.2. Yêu cầu về quản trị hệ thống của Quyết định số 1591/QĐ-BTTTT.                                                                                           |
| 4.2.1 Quản lý vận hành                                    | Tham khảo Mục II.2.1. Quản lý vận hành của Quyết định số 1591/QĐ-BTTTT. Cụ thể hóa bằng chức năng quản lý FMT_SMF.1/IPS của NIAP PP-Module.                                 |
| 4.2.2 Quản trị từ xa                                      | Tham khảo Mục II.2.2. Quản trị từ xa của Quyết định số 1591/QĐ-BTTTT.                                                                                                       |

|                                                  |                                                                                                                                                                                                                                           |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.2.2.1 Quản lý vận hành                         | Tham khảo Mục II.2.3. Quản lý xác thực và phân quyền của Quyết định số 1591/QĐ-BTTTT. Bổ sung quy định cấu hình xác thực đa yếu tố (MFA) theo tiêu chuẩn bảo mật hiện đại.                                                                |
| 4.2.2.2 Quản trị từ xa                           | Tham khảo Mục II.3. Yêu cầu về kiểm soát lỗi của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                                             |
| 4.2.2.3 Quản lý xác thực và phân quyền           | Tham khảo Mục II.3.1. Bảo vệ cấu hình của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                                                    |
| 4.2.3 Yêu cầu về kiểm soát lỗi                   | Tham khảo Mục II.3.2. Bảo vệ dữ liệu log của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                                                 |
| 4.2.3.1 Bảo vệ cấu hình                          | Tham khảo Mục II.3.3. Đồng bộ thời gian hệ thống của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                                         |
| 4.2.3.2 Bảo vệ dữ liệu nhật ký, dữ liệu ứng dụng | Tham khảo Mục II.3. Yêu cầu về kiểm soát lỗi của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                                             |
| 4.2.3.3 Đồng bộ thời gian hệ thống               | Tham khảo Mục II.6.2. Cập nhật bản và hệ thống của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                                           |
| 4.2.3.4 Sao lưu và phục hồi                      | Tham khảo Mục II.4. Yêu cầu về log của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                                                       |
| 4.2.3.5 Cập nhật bản vá hệ thống                 | Tham khảo Mục II.4.1. Log quản trị hệ thống của Quyết định số 1591/QĐ-BTTTT. Cụ thể hóa trường thông tin dựa trên tiêu chí FAU_GEN.1/IPS (Audit Data Generation) của NIAP PP-Module.                                                      |
| 4.2.4 Yêu cầu về quản lý nhật ký                 | Tham khảo Mục II.4.2. Log chức năng phát hiện và ngăn chặn xâm nhập mạng của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                 |
| 4.2.4.1 Nhật ký quản trị hệ thống                | Tham khảo Mục II.4.2. Log chức năng phát hiện và ngăn chặn xâm nhập mạng của Quyết định số 1591/QĐ-BTTTT. Cụ thể hóa các trường thông tin lưu trữ dựa trên FIP_SBD_EXT.1 và Bảng sự kiện kiểm toán (Auditable Events) của NIAP PP-Module. |

|                                                                  |                                                                                                                                                                                                              |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.2.4.2 Nhật ký cảnh báo                                         | Tham khảo Mục II.4.3. Định dạng log của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                         |
| 4.2.4.2.1 Nhật ký chức năng phát hiện và ngăn chặn xâm nhập mạng | Tham khảo Mục II.4.4. Quản lý log của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                           |
| 4.2.4.2.2 Định dạng nhật ký                                      | Tham khảo tổng quát từ Quyết định số 1591/QĐ-BTTTT và các tính năng FIP (Intrusion Prevention) của NIAP PP-Module.                                                                                           |
| 4.2.4.3 Quản lý vòng đời lưu trữ nhật ký                         | Tự xây dựng nhóm phân loại mục để làm tiêu đề.                                                                                                                                                               |
| 4.4.2 Nhật ký chức năng phát hiện và ngăn chặn xâm nhập lớp mạng | Tự xây dựng.                                                                                                                                                                                                 |
| <b>5 Yêu cầu về chức năng nghiệp vụ của nền tảng</b>             | Tự xây dựng.                                                                                                                                                                                                 |
| 5.1 Khái quát                                                    | Tham khảo Mục II.2.4. Quản lý các giao diện mạng của Quyết định số 1591/QĐ-BTTTT. Cụ thể hóa chế độ hoạt động (Promiscuous, Inline, Management) dựa trên yêu cầu FIP_NTA_EXT.1.3 của NIAP PP-Module.         |
| 5.2 Yêu cầu cụ thể                                               | Tham khảo Mục II.7.2. Hỗ trợ các giao thức mạng của Quyết định số 1591/QĐ-BTTTT. Cụ thể hóa các giao thức bắt buộc (IPv4, IPv6, ICMP, TCP, UDP) dựa trên yêu cầu FIP_NTA_EXT.1.2 của NIAP PP-Module.         |
| 5.2.1 Thu thập, tiếp nhận và mô hình hóa dữ liệu tình báo        | Tự xây dựng nhằm kiểm soát lưu lượng tại tầng ứng dụng (Lớp 7).                                                                                                                                              |
| 5.2.1.1 Quản lý các giao diện mạng                               | Tự xây dựng nhằm liên kết thông tin người dùng, thiết bị đầu cuối và định vị địa lý.                                                                                                                         |
| 5.2.1.2 Hỗ trợ các giao thức mạng                                | Tự xây dựng.                                                                                                                                                                                                 |
| 5.2.1.3 Khả năng nhận diện ứng dụng                              | Tham khảo Mục II.7.3. Phân tích thông tin trong phần tiêu đề gói tin của Quyết định số 1591/QĐ-BTTTT. Cụ thể hóa các trường Header bắt buộc kiểm tra (Version, TTL, Source/Dest Address, Checksum, Flags...) |

|                                                             |                                                                                                                                                                                                                                          |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                             | bằng yêu cầu FIP_SBD_EXT.1.1 của NIAP PP-Module.                                                                                                                                                                                         |
| 5.2.1.4 Khả năng nhận thức ngữ cảnh                         | Tham khảo Mục II.7.4. Phân tích thông tin trong phần dữ liệu gói tin của Quyết định số 1591/QĐ-BTTTT. Mở rộng dựa trên tính năng kiểm tra Payload và String-matching (FIP_SBD_EXT.1.2) cho TCP, UDP, FTP, HTTP, SMTP của NIAP PP-Module. |
| 5.2.2 Xử lý dữ liệu tình báo                                | Tham khảo Mục II.7.6. Phát hiện tấn công trên phần dữ liệu của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                              |
| 5.2.2.1 Phân tích thông tin trong phần tiêu đề gói tin      | Tham khảo yêu cầu tái tổ hợp luồng TCP, IP fragments (FIP_SBD_EXT.1.6) và kiểm tra chuẩn hóa lưu lượng (FIP_SBD_EXT.2 Traffic Normalization) của NIAP PP-Module.                                                                         |
| 5.2.2.2 Phân tích thông tin trong phần dữ liệu gói tin      | Tự xây dựng.                                                                                                                                                                                                                             |
| 5.2.2.3 Tấn công trên phần dữ liệu                          | Tham khảo Mục II.2.6. Quản lý tập luật bảo vệ của Quyết định số 1591/QĐ-BTTTT. Mở rộng bằng chức năng quản lý luật (FMT_SMF.1/IPS) của NIAP PP-Module.                                                                                   |
| 5.2.2.4 Chuẩn hóa, tái lắp ghép và chống lẫn tránh          | Tham khảo Mục II.2.7. Cập nhật tập luật bảo vệ của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                                          |
| 5.2.3 Quản lý vòng đời chỉ báo và tri thức mối đe dọa       | Tham khảo Mục II.2.8. Quản lý danh sách trắng địa chỉ IP và danh sách đen địa chỉ IP của Quyết định số 1591/QĐ-BTTTT. Cụ thể hóa dựa trên yêu cầu ngăn chặn IP (FIP_IPB_EXT.1) của NIAP PP-Module.                                       |
| 5.2.3.1 Quản lý tập luật bảo vệ                             | Tham khảo Mục II.2.9. Quản lý tập các địa chỉ IP đang bị chặn kết nối của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                   |
| 5.2.3.2 Cập nhật tập luật bảo vệ                            | Tự xây dựng để hỗ trợ tích hợp IoC.                                                                                                                                                                                                      |
| 5.2.3.3 Quản lý danh sách trắng và danh sách đen địa chỉ IP | Tham chiếu trực tiếp tính năng FIP_SBD_EXT.1 (Signature-Based IPS Functionality) của NIAP PP-Module.                                                                                                                                     |
| 5.2.3.4 Quản lý tập các địa chỉ IP đang bị chặn kết nối     | Tham chiếu trực tiếp tính năng FIP_ABD_EXT.1 (Anomaly-Based IPS Functionality) của NIAP PP-Module.                                                                                                                                       |

|                                                                           |                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.2.3.5 Tích hợp thông tin tình báo mỗi đe dọa                            | Tự xây dựng.                                                                                                                                                                                                                                                    |
| 5.2.3.6 Phát hiện tấn công dựa trên chữ ký                                | Tự xây dựng.                                                                                                                                                                                                                                                    |
| 5.2.3.7 Phát hiện dựa trên sự bất thường                                  | Tham khảo Mục II.2.10. Chia sẻ dữ liệu của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                                                                         |
| 5.2.3.8 Hỗ trợ quản lý tài sản và lỗ hổng                                 | Tự xây dựng.                                                                                                                                                                                                                                                    |
| 5.2.4 Chia sẻ, phân phối, tích hợp và kiểm soát sử dụng dữ liệu           | Tự xây dựng.                                                                                                                                                                                                                                                    |
| 5.2.4.1 Chia sẻ dữ liệu                                                   | Tự xây dựng.                                                                                                                                                                                                                                                    |
| 5.2.4.2 Tích hợp với hệ thống SIEM                                        | Tự xây dựng.                                                                                                                                                                                                                                                    |
| 5.2.4.3 Tích hợp nền tảng điều phối, tự động hóa và phản ứng an ninh mạng | Tham khảo Mục II.2.10. Chia sẻ dữ liệu của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                                                                         |
| 5.2.4.4 API và tự động hóa                                                | Tự xây dựng.                                                                                                                                                                                                                                                    |
| 5.2.4.5 Tích hợp môi trường điện toán đám mây                             | Tự xây dựng (Hỗ trợ định dạng DOCX, XLSX, PDF, HTML, XML).                                                                                                                                                                                                      |
| 5.2.4.6 Tích hợp với các hệ thống quản lý, giám sát khác                  | Tham khảo Mục II.7.1. Cơ chế thực thi bảo vệ của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                                                                   |
| 5.2.5 Thống kê xu hướng, cảnh báo và báo cáo                              | Tham khảo Mục II.7.5. Phát hiện các dạng tấn công mạng của Quyết định số 1591/QĐ-BTTTT. Cụ thể hóa thông qua danh mục tấn công tiêu chuẩn (Teardrop, Land, Ping of Death, Flooding, Scanning) của yêu cầu FIP_SBD_EXT.1.3 và FIP_SBD_EXT.1.4 từ NIAP PP-Module. |
| 5.2.5.1 Quản lý báo cáo                                                   | Tự xây dựng.                                                                                                                                                                                                                                                    |
| 5.2.5.2 Cơ chế thực thi bảo vệ                                            | Tự xây dựng.                                                                                                                                                                                                                                                    |
| 5.2.5.3 Phát hiện các dạng tấn công                                       | Tham khảo Mục II.7.7. Kiểm soát lưu lượng mạng của Quyết định số 1591/QĐ-BTTTT. Cụ thể hóa bằng các hành động ngăn chặn (Allow, Block/Drop, TCP Reset, ICMP unreachable) dựa trên yêu cầu FIP_SBD_EXT.1.5 của NIAP PP-Module.                                   |
| 5.2.5.4 Cảnh báo và kiểm soát lưu lượng mạng                              | Tự xây dựng.                                                                                                                                                                                                                                                    |

|                                                     |                                                                                                                                                                                                                                                        |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.2.5.4.1 Cảnh báo                                  | Tham khảo Mục II.5. Yêu cầu về hiệu năng xử lý của Quyết định số 1591/QĐ-BTTTT.                                                                                                                                                                        |
| 5.2.5.4.2 Kiểm soát lưu lượng mạng                  | Tham khảo Mục II.3.4. Khả năng chịu lỗi vận hành của Quyết định số 1591/QĐ-BTTTT. Cụ thể hóa thông qua cơ chế Fail-close / Fail-open và bảo toàn trạng thái theo yêu cầu FPT_FLS.1/IPS (Failure with Preservation of Secure State) của NIAP PP-Module. |
| 5.2.6 Hiệu năng xử lý, khả năng mở rộng và phục hồi | Tự xây dựng (Hỗ trợ kiến trúc Active-Active / Active-Passive).                                                                                                                                                                                         |
| 5.2.6.1 Yêu cầu về hiệu năng xử lý                  | Tự xây dựng.                                                                                                                                                                                                                                           |
| 5.2.6.2 Khả năng chịu lỗi vận hành                  | Tự xây dựng.                                                                                                                                                                                                                                           |
| 5.2.6.3 Dự phòng và tính sẵn sàng                   | Tự xây dựng.                                                                                                                                                                                                                                           |
| 5.2.6.4 Cơ chế vá lỗi ảo                            | Tham khảo Mục I.3. Khái niệm và thuật ngữ của Quyết định số 1591/QĐ-BTTTT. Bổ sung các khái niệm về chế độ hoạt động (Promiscuous, Inline) dựa trên NIAP PP-Module for IPS.                                                                            |