BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
-------	Độc lập - Tự do - Hạnh phúc

Số: 1855/QĐ-BTTTT	*Hà Nội, ngày 04 tháng 10 năm 2022*

QUYẾT ĐỊNH

BAN HÀNH YÊU CẦU KỸ THUẬT CƠ BẢN ĐỐI VỚI SẢN PHẨM KIỂM SOÁT TRUY CẬP MẠNG

BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 48/2022/NĐ-CP ngày 26 tháng 07 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Theo đề nghị của Cục trưởng Cục An toàn thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Yêu cầu kỹ thuật cơ bản đối với sản phẩm Kiểm soát truy cập mạng (Network Access Control - NAC).

Điều 2. Khuyến nghị cơ quan, tổ chức nghiên cứu, phát triển, lựa chọn, sử dụng sản phẩm NAC đáp ứng các yêu cầu kỹ thuật cơ bản theo Điều 1 Quyết định này.

Điều 3. Cục An toàn thông tin chủ trì, phối hợp với các cơ quan, tổ chức liên quan hướng dẫn việc áp dụng các yêu cầu trong Yêu cầu kỹ thuật cơ bản đối với sản phẩm NAC tại Điều 1 Quyết định này.

Điều 4. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 5. Chánh Văn phòng, Cục trưởng Cục An toàn thông tin, Thủ trưởng các đơn vị thuộc Bộ, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nơi nhận:
- Như Điều 5;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Cổng Thông tin điện tử của Bộ;
- Lưu: VT, CATTT.

Nguyễn Huy Dũng

YÊU CẦU KỸ THUẬT CƠ BẢN

ĐỐI VỚI SẢN PHẨM KIỂM SOÁT TRUY CẬP MẠNG
(Kèm theo Quyết định số 1855/QĐ-BTTTT ngày 04 tháng 10 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông)

I. THÔNG TIN CHUNG

1. Phạm vi áp dụng

Tài liệu này mô tả các yêu cầu kỹ thuật cơ bản đối với sản phẩm Kiểm soát truy cập mạng (NAC). Tài liệu bao gồm các nhóm yêu cầu: Yêu cầu về tài liệu; Yêu cầu về quản trị hệ thống; Yêu cầu về kiểm soát lỗi; Yêu cầu về log; Yêu cầu về mô hình triển khai; Yêu cầu về chức năng tự bảo vệ; Yêu cầu về chức năng kiểm soát truy cập mạng; Yêu cầu về chức năng cảnh báo và tích hợp.

2. Đối tượng áp dụng

Các cơ quan, tổ chức có liên quan đến hoạt động nghiên cứu, phát triển, đánh giá, lựa chọn sản phẩm NAC khi đưa vào sử dụng trong các hệ thống thông tin.

3. Khái niệm và thuật ngữ

Trong tài liệu này các khái niệm và thuật ngữ được hiểu như sau:

3.1. Tập luật kiểm soát kết nối trong mạng

Tập luật kiểm soát kết nối trong mạng bao gồm các tham số, quy tắc được định nghĩa và thiết lập bởi quản trị viên, cho phép NAC phát hiện, cảnh báo và thực hiện chính sách quản lý truy cập mạng nếu thông tin kết nối mạng được giám sát bởi NAC khớp luật được tạo ra.

3.2. Nhật ký hệ thống (log)

Sự kiện an toàn thông tin được hệ thống ghi lại, liên quan đến trạng thái hoạt động, thông báo, cảnh báo, sự cố, cuộc tấn công và các thông tin khác liên quan đến hoạt động của hệ thống (nếu có).

3.3. Thời gian duy trì phiên kết nối (session timeout)

Khoảng thời gian được thiết lập để cho phép hệ thống hủy phiên kết nối đối với một máy khách, nếu trong khoảng thời gian này mà hệ thống không nhận được yêu cầu mới từ máy khách đó.

3.4. Tính năng sao chép lưu lượng mạng (Port Mirroring / SPAN Port)

Tính năng trên thiết bị mạng (thường là thiết bị chuyển mạch) cho phép sao chép toàn bộ lưu lượng mạng đi qua một giao diện mạng chuyển sang một giao diện khác hoặc sang các thiết bị giám sát khác.

3.5. Kỹ thuật kiểm soát truy cập sử dụng Access Control List

Kỹ thuật kiểm soát truy cập sử dụng Access Control List cho phép thiết bị thực hiện hành động chặn hoặc cho phép kết nối mạng theo một thứ tự nhất định, dựa trên các điều kiện được cấu hình bởi quản trị viên.

3.6. Kỹ thuật yêu cầu đóng kết nối sử dụng TCP Reset

Kỹ thuật chặn kết nối mạng hoạt động dựa trên phương thức hủy kết nối của giao thức TCP với cờ Reset.

3.7. Kỹ thuật chặn kết nối mạng sử dụng ARP Poisoning

Kỹ thuật chặn kết nối mạng sử dụng ARP Poisoning cho phép NAC chuyển hướng lưu lượng của các thiết bị đầu cuối về giao diện mạng của NAC hoặc giao diện mạng của thiết bị khác để thực hiện ngăn chặn kết nối.

II. YÊU CẦU CƠ BẢN

1. Yêu cầu về tài liệu

NAC có tài liệu bao gồm các nội dung sau:

a) Hướng dẫn triển khai và thiết lập cấu hình;

b) Hướng dẫn sử dụng và quản trị.

2. Yêu cầu về quản trị hệ thống

2.1. Quản lý vận hành

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

a) Cho phép thiết lập, thay đổi, áp dụng và 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 kiểm soát kết nối trong mạng, danh sách thiết bị chuyển mạch, danh sách thiết bị đầu cuối;

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 log bằng từ khóa để xem lại;

g) Cho phép xóa log;

h) Cho phép xem thời gian hệ thống chạy tính từ lần khởi động gần nhất.

2.2. Quản trị từ xa

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

a) Sử dụng giao thức có mã hóa như TLS hoặc tương đương;

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.

2.3. Quản lý xác thực và phân quyền

NAC 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;

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) Hỗ trợ phân nhóm thiết bị và gán quyền quản trị nhóm cho các người dùng (người dùng quản trị một nhóm sẽ không thể xem và tác động lên các thiết bị trong nhóm khác).

2.4. Quản lý báo cáo

NAC 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.

2.5. Quản lý tập luật kiểm soát kết nối trong mạng

a) NAC cho phép quản lý tập luật kiểm soát kết nối trong mạng được giám sát bao gồm các thao tác sau:

i) Thêm luật mới;

ii) Sửa luật;

iii) Tìm kiếm luật;

iv) Xóa luật;

v) Kích hoạt/vô hiệu hóa luật.

b) NAC cho phép thiết lập luật để thực hiện tự động các tác vụ sau:

i) Phát hiện và thêm thiết bị mới kết nối lần đầu vào danh sách thiết bị đầu cuối;

ii) Gắn nhãn phân nhóm thiết bị;

iii) Tạo cảnh báo liên quan đến thiết bị;

iv) Chặn kết nối mạng của thiết bị;

v) Cho phép thiết bị kết nối vào mạng;

vi) Bỏ qua việc kiểm tra thiết bị.

2.6. Quản lý danh sách thiết bị chuyển mạch

NAC cho phép quản lý các thiết bị chuyển mạch đáp ứng các yêu cầu sau:

a) Cho phép giao tiếp với thiết bị thông qua các giao thức: SSH, SNMP;

b) Cho phép giám sát liên tục thông tin về trạng thái thiết bị và các cổng của thiết bị: link down, link up, link disabled/shutdown, port isolation;

c) Cho phép cấu hình đóng/mở cổng của thiết bị;

d) Cho phép cấu hình chuyển VLAN cho các cổng của thiết bị;

đ) Cho phép cấu hình bật/tắt cơ chế xác thực trên thiết bị dựa trên tiêu chuẩn quốc tế IEEE 802.1x;

e) Cho phép hỗ trợ tích hợp với các thiết bị của tối thiểu 04 hãng phổ biến.

2.7. Quản lý danh sách thiết bị đầu cuối

a) NAC cho phép quản lý danh sách thiết bị đầu cuối bao gồm các thao tác sau:

i) Thêm thiết bị mới;

ii) Sửa thông tin thiết bị;

iii) Tìm kiếm thiết bị;

iv) Xóa thiết bị;

v) Chặn kết nối mạng của thiết bị;

vi) Cho phép thiết bị kết nối vào mạng;

vii) Bỏ qua việc kiểm tra thiết bị.

b) NAC cho phép quản lý các thiết bị đầu cuối theo các trường thông tin sau:

i) Địa chỉ IP của thiết bị;

ii) Địa chỉ MAC của thiết bị;

iii) Tên nhà sản xuất thiết bị dựa trên địa chỉ MAC;

iv) Tài khoản quản trị trên thiết bị;

v) Tên thiết bị;

vi) Trạng thái quản lý thiết bị;

vii) Nhãn phân nhóm thiết bị.

2.8. Chia sẻ dữ liệu

NAC cho phép kết nối chia sẻ dữ liệu với giải pháp Quản lý và phân tích sự kiện an toàn thông tin SIEM;

3. Yêu cầu về kiểm soát lỗi

3.1. Bảo vệ cấu hình

Trong trường hợp NAC phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), NAC 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 hệ thống;

b) Cấu hình quản trị từ xa;

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

d) Tập luật kiểm soát kết nối trong mạng;

đ) Danh sách thiết bị đầu cuối;

e) Danh sách thiết bị chuyển mạch.

3.2. Bảo vệ dữ liệu log

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

3.3. Đồng bộ thời gian hệ thống

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

4. Yêu cầu về log

4.1. Log quản trị hệ thống

a) NAC cho phép ghi log 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 kiểm soát kết nối trong mạng, danh sách thiết bị chuyển mạch, danh sách thiết bị đầu cuối;

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 (link-status) của giao diện giám sát.

b) NAC cho phép ghi log quản trị hệ thống có các trường thông tin sau:

i) Thời gian sinh log (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,...).

4.2. Log cảnh báo

NAC cho phép ghi log cảnh báo được sinh ra bởi việc thực thi tập luật kiểm soát kết nối trong mạng.

4.3. Định dạng log

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

4.4. Quản lý log

NAC cho phép quản lý log 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 log (ví dụ: ngưỡng giới hạn dung lượng lưu trữ, khoảng thời gian lưu trữ,...);

b) Cho phép tìm kiếm log 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 log ra để phục vụ cho việc tích hợp các dữ liệu này vào các giải pháp về quản lý, phân tích, điều tra log.

5. Yêu cầu về mô hình triển khai

NAC cho phép triển khai theo các mô hình sau:

a) Mô hình quản lý tập trung: Nhiều thành phần giám sát thiết bị chuyển mạch, đầu cuối được triển khai phân tán trong mạng được giám sát và các thành phần này đồng bộ dữ liệu với và được quản lý bởi một thành phần quản trị tập trung;

b) Mô hình quản lý phân tán: Mỗi một thành phần giám sát có thể được triển khai và quản trị độc lập mà không bị phụ thuộc vào thành phần quản trị tập trung.

6. Yêu cầu về chức năng tự bảo vệ

6.1. Bảo vệ giao diện bên ngoài của sản phẩm

NAC có khả năng tự bảo vệ và ngăn chặn các dạng tấn công phổ biến sau vào giao diện bên ngoài của chính sản phẩm, bao gồm tối thiểu các dạng sau:

a) SQL Injection;

b) OS Command Injection;

c) XPath Injection;

d) Remote File Inclusion (RFI);

d) Local File Inclusion (LFI);

e) Cross-Site Scripting (XSS);

g) Cross-Site Request Forgery (CSRF).

6.2. Cập nhật bản vá hệ thống

NAC cho phép cập nhật bản vá để xử lý các điểm yếu, lỗ hổng bảo mật được phát hiện trên chính sản phẩm.

7. Yêu cầu về chức năng kiểm soát truy cập của thiết bị đầu cuối

7.1. Quản lý truy cập mạng theo trạng thái

NAC cho phép gán và thay đổi trạng thái quản lý các thiết bị đầu cuối theo các trường hợp sau:

a) Được phép truy cập vào mạng (permitted);

b) Bị hạn chế truy cập vào mạng nhưng vẫn có thể được truy cập bởi các máy chủ quản trị để khắc phục các lỗi cơ bản (restricted);

c) Bị chặn toàn bộ kết nối truy cập vào mạng (blocked);

d) Mới phát hiện có kết nối nhưng chưa được quản lý và không được phép truy cập vào mạng (un-managed).

7.2. Kiểm soát truy cập mạng theo nhiều phương thức

NAC cho phép kiểm soát trực tiếp hoặc tương tác với thiết bị mạng/thiết bị bảo mật để thực hiện quản lý truy cập mạng thông qua tối thiểu 01 trong các kỹ thuật sau:

a) Kỹ thuật kiểm soát truy cập sử dụng Access Control List;

b) Kỹ thuật yêu cầu đóng kết nối sử dụng TCP Reset;

c) Kỹ thuật chặn kết nối mạng sử dụng ARP Poisoning.

8. Yêu cầu về chức năng cảnh báo và tích hợp

8.1. Cảnh báo theo thời gian thực

NAC cho phép tự động cảnh báo tới người dùng theo thời gian thực đối với các loại sự kiện sau:

a) Có thiết bị đầu cuối mới truy cập vào mạng;

b) Có thiết bị đầu cuối chuyển vùng mạng;

c) Có thiết bị chuyển mạch bị mất kết nối;

d) Có sự gián đoạn đối với tính năng sao chép lưu lượng mạng.

8.2. Cảnh báo theo nhiều phương thức

NAC cho phép tự động cảnh báo theo các phương thức sau:

a) Hiển thị nội dung cảnh báo trên giao diện đồ họa về quản lý cảnh báo;

b) Cảnh báo thông qua tối thiểu 02 phương thức: gửi thư điện tử, gửi tin nhắn SMS, gửi tin nhắn qua ứng dụng truyền tin.

8.3. Hỗ trợ tích hợp API

NAC cho phép thiết lập cấu hình API để các ứng dụng, hệ thống, giải pháp khác tương tác và thực hiện các thao tác sau:

a) Tìm kiếm thiết bị theo địa chỉ IP hoặc địa chỉ MAC;

b) Chặn kết nối mạng của thiết bị;

c) Cho phép thiết bị kết nối vào mạng;

d) Bỏ qua việc kiểm tra thiết bị./.