BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 1844/QĐ-BTTTT	*Hà Nội, ngày 18 tháng 11 năm 2021*

QUYẾT ĐỊNH
Ban hành Yêu cầu kỹ thuật cơ bản đối với sản phẩm Mạng riêng ảo

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 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 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 Mạng riêng ảo (Virtual Private Network - VPN).

Điều 2. Khuyến nghị cơ quan, tổ chức nghiên cứu, phát triển, lựa chọn, sử dụng sản phẩm VPN 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 VPN 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./.

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

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Huy Dũng

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

YÊU CẦU KỸ THUẬT CƠ BẢN ĐỐI VỚI SẢN PHẨM MẠNG RIÊNG ẢO

(Kèm theo Quyết định số 1844/QĐ-BTTTT ngày 18 tháng 11 năm 2021 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 Mạng riêng ảo (Virtual Private Network - VPN). 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 hiệu năng xử lý, Yêu cầu về chức năng tự bảo vệ, Yêu cầu về dịch vụ mạng riêng ảo dựa trên giao thức SSL/TLS, Yêu cầu về dịch vụ mạng riêng ảo dựa trên giao thức IPSec.

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 VPN 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. 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, thông tin về các mối đe dọa thu thập được và các thông tin khác liên quan đến hoạt động của hệ thống (nếu có).

3.2. 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.

3.3. Đường hầm (tunnel)

Kênh kết nối logic cho phép đóng gói và mã hóa dữ liệu khi đi qua mạng riêng ảo.

3.4. Cơ chế Split Tunneling

Cơ chế định tuyến lưu lượng cho phép xác định lưu lượng nào đi qua mạng riêng ảo và lưu lượng nào đi qua mạng cục bộ, tùy thuộc theo cấu hình mạng riêng ảo đang được áp dụng.

3.5. Cơ chế Reverse Proxy

Cơ chế triển khai VPN cho phép sử dụng máy chủ trung gian (proxy), đứng giữa máy chủ cung cấp dịch vụ và máy trạm yêu cầu dịch vụ để kiểm soát và chuyển tiếp lưu lượng từ máy trạm (nếu hợp lệ) đến máy chủ thích ứng.

3.6. Kiểm tra trạng thái hoạt động (liveness check)

Việc thực hiện kiểm tra xem một thiết bị/phần mềm VPN còn hoạt động hay không, thông qua cơ chế gửi gói tin xác nhận giữa hai thiết bị/phần mềm VPN.

3.7. Thỏa thuận bảo mật (security association)

Tập các thỏa thuận (các thông tin về thuật toán, khóa mật mã và các tham số, điều kiện khác) được thiết lập thông qua quá trình trao đổi ban đầu để phục vụ việc thiết lập kết nối mạng riêng ảo giữa các thiết bị/phần mềm VPN ngang hàng (được gọi là peer).

3.8. Bên khởi tạo (initiator)

Thiết bị/phần mềm VPN ngang hàng thực hiện việc gửi yêu cầu khởi tạo phiên kết nối mạng riêng ảo.

3.9. Bên phản hồi (responder)

Thiết bị/phần mềm VPN ngang hàng thực hiện việc trả lời yêu cầu khởi tạo phiên kết nối mạng riêng ảo được gửi từ bên khởi tạo.

II. YÊU CẦU CƠ BẢN

1. Yêu cầu về tài liệu

VPN 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

VPN 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 mạng riêng ảo, cấu hình tài khoản xác thực và phân quyền người dùng;

b) Cho phép cấu hình thời gian duy trì phiên kết nối quản trị từ xa;

c) Cho phép thiết lập, thay đổi các tham số giới hạn đối với kết nối quản trị từ xa tối thiểu cho phép giới hạn địa chỉ IP, giới hạn số phiên kết nối quản trị đồng thời;

d) Cho phép đăng xuất tài khoản người dùng có phiên kết nối quản trị từ xa còn hiệu lực;

đ) Cho phép tìm kiếm dữ liệu log bằng từ khóa để xem lại.

2.2. Quản trị từ xa

VPN 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

VPN 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 tối thiểu 01 giao thức cung cấp dịch vụ xác thực: RADIUS, LDAPS, Active Directory;

c) 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.

3. Yêu cầu về kiểm soát lỗi

3.1. Bảo vệ cấu hình

Trong trường hợp VPN phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), VPN 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 mạng riêng ảo;

d) Cấu hình tài khoản xác thực và phân quyền người dùng.

3.2. Đồng bộ thời gian hệ thống

Trong trường hợp VPN phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), VPN 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) VPN 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 mạng riêng ảo, cấu hình tài khoản xác thực và phân quyền người dùng;

iv) Khởi tạo kết nối mạng riêng ảo;

v) Hủy bỏ phiên kết nối mạng riêng ảo.

b) VPN 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 dịch vụ,...);

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. Định dạng log

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

4.3. Quản lý log

VPN cho phép quản lý log đáp ứng các yêu cầu sau:

a) 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);

b) 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 hiệu năng xử lý

5.1. Đối với việc áp dụng các sự thay đổi trong các cấu hình

VPN cho phép áp dụng các sự thay đổi trong các cấu hình mà không làm gián đoạn hoạt động dịch vụ mạng riêng ảo quá 01 phút.

6. Yêu cầu về chức năng tự bảo vệ

6.1. Phát hiện và ngăn chặn tấn công hệ thống

VPN có khả năng tự bảo vệ, ngăn chặn các dạng tấn công phổ biến sau vào giao diện ra bên ngoài của hệ thống, bao gồm tối thiểu các dạng sau:

a) SQL Injection;

b) OS Command Injection;

c) XPath Injection;

d) Remote File Inclusion (RFI);

đ) Local File Inclusion (LFI);

e) Cross-Site Scripting (XSS);

g) Cross-Site Request Forgery (CSRF);.

6.2. Cập nhật bản vá hệ thống

VPN có chức năng cho phép cập nhật bản vá để xử lý các điểm yếu, lỗ hổng bảo mật.

7. Yêu cầu về dịch vụ mạng riêng ảo dựa trên giao thức SSL/TLS

7.1. Quản lý thiết lập giao thức mã hóa kênh truyền

VPN có chức năng cho phép quản lý thiết lập giao thức mã hóa kênh truyền SSL và TLS đối với các phiên kết nối mạng riêng ảo đáp ứng các yêu cầu sau:

a) Hỗ trợ nhiều phiên bản, trong đó tối thiểu phải hỗ trợ phiên bản TLS v1.3 (RFC 8446);

b) Cho phép vô hiệu hóa các phiên bản thấp hơn TLS v1.3, trong đó bao gồm các phiên bản của giao thức SSL.

7.2. Quản lý thiết lập bộ mật mã

VPN có chức năng cho phép quản lý thiết lập bộ mật mã đối với các phiên kết nối mạng riêng ảo đáp ứng các yêu cầu sau:

a) Hỗ trợ nhiều các bộ mật mã khác nhau, trong đó, tối thiểu phải hỗ trợ bộ mật mã TLS_AES_256_GCM_SHA384;

b) Cho phép vô hiệu hóa các bộ mật mã yếu hơn hoặc bị công bố có lỗ hổng, điểm yếu đã biết dựa trên tiêu chuẩn chung trong nước hoặc quốc tế.

7.3. Quản lý chứng thư số

VPN có chức năng cho phép quản lý chứng thư số đối với các phiên kết nối mạng riêng ảo đáp ứng các yêu cầu sau:

a) Cho phép đăng ký mới chứng thư số gắn liền với thiết bị đăng ký;

b) Cho phép cài đặt chứng thư số;

c) Cho phép gia hạn chứng thư số;

d) Cho phép thay thế chứng thư số;

đ) Cho phép xem thông tin chi tiết của chứng thư số bao gồm tối thiểu các trường thông tin sau:

i) Số hiệu (serial number);

ii) Tên chủ thể (subject name);

iii) Tên tổ chức cấp chứng thư số (issuer name);

iv) Thời hạn còn hiệu lực (validity dates);

v) Phần mở rộng X.509 (X.509 extensions);

e) Cho phép tra cứu trạng thái thu hồi của chứng thư số bằng 01 trong các cách thức sau:

i) Dựa trên danh sách chứng thư số đã bị thu hồi (CRL) được tải về trực tuyến qua giao thức LDAP hoặc HTTP;

ii) Thông qua giao thức OCSP (RFC 6960).

7.4. Xác thực chứng thư số

a) Trước khi khởi tạo các phiên kết nối mạng riêng ảo, nếu hỗ trợ kiểm tra tính hợp lệ của chứng thư số của máy trạm, máy chủ VPN cho phép sinh cảnh báo và cho phép từ chối khởi tạo kết nối trong các trường hợp sau:

i) Chứng thư số không được ký bởi tổ chức cấp chứng thư số tin cậy;

ii) Chứng thư số hết hạn;

iii) Chứng thư số đã bị thu hồi;

iv) Chứng thư số không có thông tin về nguồn tin cậy cung cấp dịch vụ tra cứu trạng thái thu hồi;

v) Chứng thư số không trùng khớp với các thông tin của máy trạm.

b) Trước khi khởi tạo các phiên kết nối mạng riêng ảo, máy trạm VPN kiểm tra tính hợp lệ của chứng thư số của máy chủ, và cho phép sinh cảnh báo và cho phép từ chối khởi tạo kết nối trong các trường hợp sau:

i) Chứng thư số không được ký bởi tổ chức cấp chứng thư số tin cậy;

ii) Chứng thư số hết hạn;

iii) Chứng thư số đã bị thu hồi;

iv) Chứng thư số không trùng khớp với các thông tin của máy chủ.

7.5. Quản lý thiết lập vận hành dịch vụ

VPN cho phép quản lý thiết lập vận hành dịch vụ đáp ứng tối thiểu 01 trong 02 nhóm yêu cầu sau:

a) Nếu hỗ trợ cơ chế Split Tunneling thì đáp ứng các yêu cầu sau:

i) Cho phép kích hoạt/vô hiệu hóa cơ chế này;

ii) Tích hợp các biện pháp ngăn chặn việc vượt qua sự kiểm soát của đường hầm khi cơ chế này được kích hoạt;

b) Nếu hỗ trợ cơ chế Reverse Proxy thì đáp ứng các yêu cầu sau:

i) Tích hợp cơ chế sửa đổi thông tin trên URL;

ii) Cho phép xóa các thông tin nhạy cảm (nếu có) về các phiên kết nối mạng riêng ảo còn được lưu trên máy trạm (bao gồm thông tin xác thực người dùng, thông tin tự động hoàn thành biểu mẫu, dữ liệu bộ nhớ đệm, dữ liệu lịch sử hoạt động);

iii) Cho phép thiết lập tự động hủy bỏ phiên kết nối mạng riêng ảo khi người dùng không tương tác trong một khoảng thời gian nhất định.

7.6. Hỗ trợ giao thức IPv6

VPN cho phép vận hành tương thích với giao thức IPv6.

8. Yêu cầu về dịch vụ mạng riêng ảo dựa trên giao thức IPSec

8.1. Quản lý thiết lập giao thức thống nhất thỏa thuận bảo mật

VPN cho phép quản lý thiết lập giao thức thống nhất thỏa thuận bảo mật IKEv2 đáp ứng các yêu cầu sau:

a) Cho phép xác thực bằng các phương thức sau:

i) Khóa bí mật trao đổi trước (pre-shared key);

ii) Thuật toán RSA với độ dài khóa 2048 bit và hàm băm SHA2-256.

b) Hỗ trợ các thuật toán mật mã sau (RFC 8247):

i) ENCR_AES_CBC;

ii) PRF_HMAC_SHA2_256;

iii) AUTH_HMAC_SHA2_256_128;

iv) Diffie-Hellman Group 14.

c) Hỗ trợ tối thiểu 01 trong các loại ID sau đối với giai đoạn 1:

i) ID_IPV4_ADDR;

ii) ID_DER_ASN1_DN;

iii) ID_FQDN;

iv) ID_RFC822_ADDR.

d) Cho phép phản hồi hợp lệ khi được kiểm tra trạng thái hoạt động;

e) Cho phép lắng nghe trên cổng có số hiệu khác 500 và 4500.

8.2. Quản lý thiết lập giao thức mã hóa kênh truyền

VPN cho phép quản lý thiết lập giao thức mã hóa kênh truyền IPSec đáp ứng các yêu cầu sau:

a) Hỗ trợ giao thức ESP vận hành theo chế độ đường hầm;

b) Hỗ trợ các thuật toán mật mã sau:

i) AES-CBC-256 (RFC 3602);

ii) PRF_HMAC_SHA2_256 (RFC 4868).

c) Tích hợp các biện pháp chống tấn công phát lại (replay attack).

8.4. Quản lý chứng thư số

VPN có chức năng cho phép quản lý chứng thư số đối với các phiên kết nối mạng riêng ảo đáp ứng các yêu cầu sau:

a) Cho phép đăng ký mới chứng thư số gắn liền với thiết bị đăng ký;

b) Cho phép cài đặt chứng thư số;

c) Cho phép gia hạn chứng thư số;

d) Cho phép thay thế chứng thư số;

đ) Cho phép xem thông tin chi tiết của chứng thư số bao gồm tối thiểu các trường thông tin sau:

i) Số hiệu (serial number);

ii) Tên chủ thể (subject name);

iii) Tên tổ chức cấp chứng thư số (issuer name);

iv) Thời hạn còn hiệu lực (validity dates);

v) Phần mở rộng X.509 (X.509 extensions);

e) Cho phép tra cứu trạng thái thu hồi của chứng thư số bằng 01 trong các cách thức sau:

i) Tra cứu dựa trên danh sách chứng thư số đã bị thu hồi (CRL) được tải về trực tuyến qua giao thức LDAP hoặc HTTP;

ii) Tra cứu thông qua giao thức OCSP (RFC 6960).

8.5. Xác thực chứng thư số

Trước khi khởi tạo các phiên kết nối mạng riêng ảo, thiết bị/phần mềm VPN

ngang hàng kiểm tra tính hợp lệ của chứng thư số của bên gửi, và cho phép sinh cảnh báo và từ chối khởi tạo kết nối trong các trường hợp sau:

a) Chứng thư số không được ký bởi tổ chức cấp chứng thư số tin cậy;

b) Chứng thư số hết hạn;

c) Chứng thư số đã bị thu hồi;

d) Chứng thư số không trùng khớp với các thông tin của bên gửi.

8.6. Quản lý thiết lập vận hành dịch vụ

VPN cho phép quản lý thiết lập vận hành dịch vụ đáp ứng các yêu cầu sau:

a) Hoạt động trong trường hợp địa chỉ IP được cấp phát động;

b) Nếu sản phẩm có hỗ trợ triển khai phần mềm máy trạm truy cập từ xa dịch vụ mạng riêng ảo (IRAC) thì các yêu cầu sau phải được đáp ứng:

i) IRAC chỉ cho phép thực hiện vai trò bên khởi tạo trong quá trình thống nhất thỏa thuận bảo mật ban đầu;

ii) IRAC cho phép thực hiện cả vai trò bên khởi tạo và bên phản hồi trong quá trình sinh lại khóa mật mã (rekey) dùng trong kết nối mạng riêng ảo;

iii) IRAC hỗ trợ tương thích với giao thức NAT (RFC 3947, RFC 3948);

iv) IRAC cho phép giao tiếp bằng giao thức IKEv2 trong trường hợp gói tin đến có có số hiệu cổng nguồn bất kỳ;

v) IRAC đáp ứng tất cả các yêu cầu ở II.1, II.3, II.4 (ngoại trừ II.4.1.a.i, II.4.1.a.ii, II.4.1.a.iii, II.4.3.a), II.5, II.6, II.8 (ngoại trừ II.8.1.a.i, II.8.6.a).

8.7. Hỗ trợ giao thức IPv6

VPN cho phép vận hành tương thích với giao thức IPv6.