Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Giới thiệu chung về dự toán mua sắm, gói thầu:

- Tên gói thầu: Gia hạn bản quyền các phần mềm cài trên thiết bị (tường lửa, cân bằng tải), thời gian gia hạn 01 năm - bắt đầu từ 29/12/2025 đến hết 29/12/2026.

- Tên dự toán mua sắm: Tuyên truyền về các lĩnh vực thuộc phạm vi quản lý của Cục Quản lý và Phát triển thị trường trong nước trên các cơ quan thông tấn, báo chí năm 2025; nhiệm vụ gia hạn bản quyền các phần mềm cài trên thiết bị.

- Hình thức lựa chọn nhà thầu: Chào hàng cạnh tranh trong nước.

- Phương thức lựa chọn nhà thầu: Một giai đoạn, một túi hồ sơ.

- Thời gian bắt đầu tổ chức lựa chọn nhà thầu: Quý III năm 2025

- Loại hợp đồng: Trọn gói.

- Thời gian thực hiện gói thầu: 03 tháng.

- Thời gian thực hiện hợp đồng: 12 tháng (01 năm), bắt đầu từ 29/12/2025 đến hết 29/12/2026

2. Hiện trạng hạ tầng kỹ thuật và thiết bị

Xem chi tiết thông tin tại *Phụ lục: Thông tin về hạ tầng CNTT và thiết bị* trong E-HSMT

3. Mục tiêu công việc:

- Thuê đơn vị Gia hạn bản quyền các phần mềm cài trên thiết bị (tường lửa, cân bằng tải) cho Cục Quản lý và Phát triển thị trường trong nước.

- Đảm bảo các thiết bị được gia hạn bản quyền sử dụng các phần mềm, dịch vụ bảo hành, bảo trì, hỗ trợ kỹ thuật từ hãng sản xuất thiết bị và nhà thầu

- Đảm bảo thiết bị hoạt động ổn định thường xuyên liên tục (24/7)

- Đảm bảo an ninh an toàn thông tin, bảo vệ hệ thống trước các nguy cơ, tấn công và các yếu tố gây ảnh hưởng đến hoạt động của thiết bị

- Đáp ứng các yêu cầu về quản trị, vận hành, hiệu quả sử dụng của thiết bị;

- Hỗ trợ bồi dưỡng, nâng cao kiến thức và kỹ năng quản trị, sử dụng thiết bị cho người dùng

4. Yêu cầu kỹ thuật của gói thầu:

4.1. Yêu cầu chung

Nhà thầu phải đáp ứng và cung cấp đầy đủ các tài liệu để chứng minh về mức độ phù hợp, tương thích và sẵn sàng của dịch vụ như sau:

TT	Tên/nội dung	Yêu cầu về tài liệu kèm theo E-HSDT để chứng minh
1	- Đổi thiết bị (1 đổi 1) nếu có các thiết bị, linh kiện hư hỏng do lỗi của nhà sản xuất nhưng không thể sửa chữa,	Cam kết của hãng sản xuất hoặc nhà phân phối hoặc đại diện chính thức của hãng sản xuất tại Việt

TT	Tên/nội dung	Yêu cầu về tài liệu kèm theo E-HSDT để chứng minh
	khắc phục. - Sản phẩm, dịch vụ chào thầu có các tính năng bảo đảm an ninh an toàn thông tin, giúp ngăn ngừa, phòng chống các cuộc tấn công, mã độc, phá hoại hệ thống. - Sản phẩm, dịch vụ chào thầu là sản phẩm dịch vụ do chính hãng sản xuất cung cấp. - Hàng hóa, dịch vụ chào thầu chưa có kế hoạch ngừng cung cấp (EOL) trong năm 2026. - Hỗ trợ cho khách hàng (chủ đầu tư, bên mời thầu hoặc đơn vị sử dụng) mượn thiết bị tương đương để sử dụng trong thời gian thiết bị thực hiện bảo hành, sửa chữa, khắc phục lỗi hỏng hóc, sự cố nếu tại thời điểm đó hãng sản xuất hoặc đơn vị phân phối chính thức có sẵn thiết bị ở Việt Nam.	Nam. (Nếu tài liệu là tiếng nước ngoài thì phải trình bày song ngữ hoặc kèm bản dịch ra tiếng Việt)
2	Cung cấp tài liệu kỹ thuật (Specification/Catalogue/Datasheet hoặc tài liệu tương đương) chính hãng sản xuất để làm cơ sở tham chiếu, chứng minh tính đáp ứng các yêu cầu về tiêu chuẩn thực hiện dịch vụ do nhà thầu đề xuất.	- Tài liệu tham chiếu có xác nhận của hãng sản xuất, đại diện chính thức hoặc đơn vị phân phối được hãng sản xuất ủy quyền chính thức tại Việt Nam. *hoặc* - Chỉ rõ địa chỉ tham chiếu chi tiết trên website chính thức của hãng sản xuất
3	Trường hợp nhà thầu không phải là hãng sản xuất thì nhà thầu phải chứng minh là đối tác và được hãng sản xuất ủy quyền để tham gia (thực hiện) gói thầu	Tài liệu chứng minh nhà thầu là đối tác được ủy quyền tham gia (thực hiện) gói thầu của hãng sản xuất (nếu tài liệu là tiếng nước ngoài thì phải trình bày song ngữ hoặc kèm bản dịch ra tiếng Việt)

4.2. Yêu cầu về danh mục thiết bị cần thực hiện

Bản quyền gia hạn cập nhật phần mềm và hỗ trợ kỹ thuật, bảo trì, bảo hành, duy trì, giám sát hoạt động cho các thiết bị sau:

TT	Danh mục thiết bị	Ký mã hiệu, nhãn mác	SL	ĐVT
1	Thiết bị tường lửa	Fortigate FG-601E, Fortinet	2	Chiếc
2	Thiết bị cân bằng tải ứng dụng	FortiADC FAD-400F, Fortinet	2	Bộ

4.3. Yêu cầu về tiêu chuẩn thực hiện dịch vụ

4.3.1 Bản quyền gia hạn cập nhật phần mềm cho các thiết bị

Bản quyền gia hạn cập nhật phần mềm cho các thiết bị phải đáp ứng đầy đủ các tính năng, dịch vụ và tiêu chuẩn theo yêu cầu sau:

TT	Tên dịch vụ	Yêu cầu
1	**Bản quyền gia hạn cập nhật phần mềm cho thiết bị tường lửa**	Thiết bị **Fortinet FortiGate FG-601E**: số lượng: 02 chiếc, thời hạn tối thiểu 1 năm (tối thiểu 12 tháng hoặc đến hết ngày 31/12/2026 kể từ ngày kích hoạt dịch vụ (hoặc giấy phép, bản quyền))
	Bao gồm các tính năng	- IPS: + IPS: cung cấp khả năng năng phát hiện và phân tích giao thức dựa trên chữ ký (signature) để xác định và chặn lưu lượng truy cập độc hại, tăng cường bảo mật mạng và ứng phó với mối đe dọa + URL Độc hại (Malicious/Botnet URLs): cập nhật Cơ sở dữ liệu về URL để phát hiện tấn công khai thác, cập nhật các chữ ký (signature) IPS về các URL độc hại đã biết, cho phép phát hiện và chặn các mối đe dọa dựa trên web, bao gồm cả thông tin liên lạc C&C của botnet và tải xuống phần mềm độc hại
		- Bảo vệ phần mềm độc hại nâng cao (Advanced Malware Protection - AMP): + Antivirus: Chữ ký (signature) chống virus (Antivirus signatures) và bản cập nhật công cụ cung cấp thông tin cập nhật thường xuyên về các mẫu virus và phần mềm độc hại đã biết, cho phép phát hiện và ngăn chặn các mối đe dọa trong thời gian thực + Phần mềm độc hại di động: Phát hiện và chặn các mối đe dọa phần mềm độc hại đối với thiết bị di động, sử dụng tính năng phát hiện và phân tích hành vi dựa trên chữ ký (signature) để bảo vệ các thiết bị này và ngăn chặn vi phạm dữ liệu + Bảo vệ chống sự bùng phát virus: Tăng cường bảo vệ chống virus bằng cách truy vấn chữ ký (signature) băm phần mềm độc hại từ máy chủ Global Threat Intelligence của FortiGuard, cho phép phát hiện mối đe dọa zero-day theo thời gian thực trước khi chữ ký (signature) đến + Phát hiện virus dựa trên AI: Công cụ AV heuristic cập nhật sử dụng thuật toán học máy để phát hiện phần mềm độc hại không xác định,

TT	Tên dịch vụ	Yêu cầu
		phân tích hành vi và đặc điểm của tệp để xác định và chặn các mối đe dọa trong thời gian thực, tăng cường bảo vệ chống virus + FortiGate Cloud Sandbox: Gửi tệp để phát hiện mối đe dọa nâng cao, phân tích tệp và URL trong môi trường dựa trên đám mây, sử dụng phân tích hành vi và học máy để xác định các mối đe dọa chưa xác định
		- Lọc URL, DNS & Video: + Lọc URL: Phân loại hàng tỷ trang web, cho phép người dùng chặn hoặc cho phép truy cập, với hơn ≥ 45 triệu xếp hạng trang web, nâng cao tính năng lọc web và cung cấp bảo vệ thời gian thực + Lọc DNS: Chặn các miền độc hại và áp dụng tính năng lọc dựa trên danh mục, sử dụng cơ sở dữ liệu rộng lớn về các miền độc hại và không mong muốn đã biết để ngăn chặn các mối đe dọa dựa trên DNS và thực thi các chính sách sử dụng internet + Lọc Video: Phân loại và chặn quyền truy cập vào video dựa trên danh mục FortiGuard, cho phép kiểm soát nội dung video, bao gồm YouTube và các nền tảng video khác, để thực thi các chính sách sử dụng internet + Chứng chỉ độc hại: Gói động duy trì danh sách đen chứng chỉ dựa trên dấu vân tay, cho phép chặn giao tiếp botnet sử dụng SSL, giúp ngăn chặn các nỗ lực vượt qua phần mềm độc hại và IPS
		- Lọc thư, chống thư rác: Kết nối máy chủ FortiGuard để giúp xác định địa chỉ IP hoặc email của người gửi thư rác, URL lừa đảo đã biết, URL rác đã biết, kiểm tra mã băm của email rác đã biết
		- FortiCare Premium: + RMA (Return Merchandise Authorization - trả lại hàng đã được ủy quyền): Hỗ trợ bảo hành phần cứng với dịch vụ thay thế nâng cao (Advanced Replacement): Hãng sản xuất gửi thiết bị thay thế thiết bị lỗi trước khi nhận được thiết bị lỗi từ phía khách hàng + Hỗ trợ kỹ thuật qua web + Hỗ trợ kỹ thuật qua điện thoại + Cập nhật Firmware

TT	Tên dịch vụ	Yêu cầu
		+ Công cụ hỗ trợ trực tuyến: Có + Cổng quản lý thiết bị (Asset Management Portal) + Thời gian phản hồi (sự cố quan trọng): ≤ 1 giờ + Thời gian phản hồi (sự cố không quan trọng): Trong ngày làm việc tiếp theo
		- Dịch vụ cập nhật được hỗ trợ theo gói FortiCare: + Kiểm soát ứng dụng: Sử dụng để xác định các ứng dụng có chữ ký (signature) chính xác, cho phép thực thi chính sách chi tiết, bảo mật được cải thiện và hiệu suất mạng được tối ưu hóa, bao gồm nhiều ứng dụng và giao thức + Inline CASB: Hỗ trợ các định nghĩa cập nhật theo thời gian thực hồ sơ bảo mật Inline CASB được sử dụng trong các chính sách tường lửa để hỗ trợ khả năng hiển thị, kiểm soát và bảo mật cho các ứng dụng dựa trên đám mây + Phát hiện thiết bị/hệ điều hành: Cho phép FortiOS giám sát mạng và thu thập thông tin về các thiết bị hoạt động trên các mạng đó. Những thông tin này sau đó được cung cấp trên GUI, cung cấp khả năng hiển thị chi tiết cho người dùng + Kiểm tra PSIRT: Nâng cao xếp hạng bảo mật với gói tiện ích bổ sung này, xác định các lỗ hổng PSIRT của các thiết bị Fabric được kết nối, sau đó khuyến khích quản trị viên cập nhật mọi thiết bị bị ảnh hưởng
2	**Bản quyền gia hạn cập nhật phần mềm cho thiết bị cân bằng tải ứng dụng**	Thiết bị **Fortinet FortiADC 400F**: số lượng: 02 chiếc, thời hạn tối thiểu 1 năm (tối thiểu 12 tháng hoặc đến hết ngày 31/12/2026 kể từ ngày kích hoạt dịch vụ (hoặc giấy phép, bản quyền))
	Bao gồm các dịch vụ	- IP Reputation: thông tin tổng hợp danh sách về các IP nguồn độc hại được cập nhật liên tục theo thời gian thực, nâng cao bảo mật chủ động ngăn chặn trước các cuộc tấn công
		- Dịch vụ Antivirus: Tự động cập nhật các signature mới nhất về các loại virus, spyware, malware đã biết, phát hiện và ngăn chặn các mối đe dọa trong thời gian thực
		- Intrusion Prevention (IPS): được AI/ML hỗ trợ, cập nhật các quy tắc ngăn chặn xâm nhập theo

TT	Tên dịch vụ	Yêu cầu
		thời gian thực, giúp phát hiện và ngăn chặn các mối đe dọa đã biết, tăng cường bảo mật
		- WAF Security gồm WAF Signatures và Adaptive Learning: + Cung cấp tính năng AL (Adaptive Learning giúp phân tích tự động các truy cập của thiết bị mạng trong hệ thống (máy tính của người dùng, máy chủ) để xây dựng các chính sách ngăn chặn các cuộc tấn công Web xảy ra. + Cung cấp các chữ ký (signature) mở rộng so với cơ sở dữ liệu hiện có trên thiết bị, đảm bảo chống lại được các tấn công, lỗ hổng hàng đầu nằm trong OWASP Top 10.
		- Credential Stuffing Defense: luôn cập nhật cơ sở dữ liệu về các thông tin xác thực đã bị đánh cắp + Xác định các nỗ lực đăng nhập bằng các thông tin đăng nhập đã bị đánh cắp từ nhiều nguồn + Hỗ trợ ngăn chặn các cuộc tấn công bằng thông tin xác thực đã bị đánh cắp
		Sandbox Cloud: hỗ trợ phát hiện các mối đe dọa nâng cao, phát hiện các malware chưa được biết tới trước đó
		Data Loss Prevention – DLP: + Xác định và theo dõi dữ liệu của tổ chức, bảo vệ chống lại các vi phạm dữ liệu, các mối đe dọa và đánh cắp dữ liệu + Quản lý tập trung và bảo mật các mẫu dữ liệu nhạy cảm được xác định trước với các mẫu kiểu dữ liệu như mã số thuế, số thẻ tín dụng, giấy phép lái xe, … + Ngăn chặn thất thoát dữ liệu và đảm bảo tuân thủ chính sách về bảo mật dữ liệu như CCPA, PCI-DSS, GDPR và HIPAA.
		FortiCare Premium: + RMA (Return Merchandise Authorization - trả lại hàng đã được ủy quyền): Hỗ trợ bảo hành phần cứng với dịch vụ thay thế nâng cao (Advanced Replacement): Hãng sản xuất gửi thiết bị thay thế thiết bị lỗi trước khi nhận được thiết bị lỗi từ phía khách hàng + Hỗ trợ kỹ thuật qua web + Hỗ trợ kỹ thuật qua điện thoại

TT	Tên dịch vụ	Yêu cầu
		+ Cập nhật Firmware + Công cụ hỗ trợ trực tuyến: Có + Cổng quản lý thiết bị (Asset Management Portal) + Thời gian phản hồi (Sự cố quan trọng): ≤ 1 giờ + Thời gian phản hồi (Sự cố không quan trọng): Trong ngày làm việc tiếp theo

4.3.2 Hỗ trợ kỹ thuật, bảo trì, bảo hành, duy trì, giám sát hoạt động

Dịch vụ hỗ trợ kỹ thuật, bảo trì, bảo hành, duy trì, giám sát hoạt động của các thiết bị phải đáp ứng đầy đủ các yêu cầu sau

TT	Nội dung yêu cầu	Yêu cầu
1	Cập nhật phần mềm	Thiết bị phải được cập nhật thường xuyên, liên tục các phiên bản phần mềm (hệ điều hành, danh mục, dữ liệu bổ sung...) mới nhất do nhà sản xuất phát hành
2	Sửa chữa, khắc phục sự cố	Thiết bị phải được sửa chữa, khắc phục sự cố, lỗi, hư hỏng. Hiệu chỉnh các sai lệch nhanh chóng, kịp thời theo đúng quy trình và tiêu chuẩn của nhà sản xuất
3	Bảo hành	Thiết bị phải được nhà thầu triển khai áp dụng các nội dung, quy trình và chế độ bảo hành theo tiêu chuẩn của Nhà sản xuất tương ứng với gói dịch vụ chào thầu
4	Phòng ngừa chủ động	Thiết bị phải được kiểm tra, bảo trì, bảo dưỡng theo quy trình, thời hạn, tiêu chuẩn của nhà sản xuất Nhà thầu phải có các biện pháp phòng ngừa chủ động, giảm thiểu tối đa các rủi ro, nguy cơ về lỗi, hỏng hóc, sự cố làm ảnh hưởng đến hoạt động của thiết bị
5	Giám sát hoạt động	Các thiết bị phải được giám sát, cung cấp thông tin về tình trạng hoạt động, tính năng vận hành, dự báo về các rủi ro, nguy cơ tiềm ẩn một cách đầy đủ, kịp thời
6	Tư vấn, hỗ trợ kỹ thuật	Thiết bị phải được nhà thầu lắp đặt, cài đặt, thiết lập tham số, cập nhật phần mềm, dữ liệu khi chủ đầu tư có nhu cầu về chuyển đổi hệ thống, thay đổi vị trí, địa điểm vận hành; sửa đổi kiến trúc, giải pháp kỹ thuật, cách thức, phương thức vận hành kết nối; Người dùng phải luôn được hỗ trợ, tư vấn, trả lời các câu hỏi, giải đáp các thắc mắc, đáp ứng yêu

TT	Nội dung yêu cầu	Yêu cầu
		cầu về đào tạo, hướng dẫn, bổ sung kiến thức, kỹ năng trong quá trình quản trị, sử dụng

4.4. Yêu cầu về thời gian

4.4.1 Bản quyền gia hạn cập nhật phần mềm cho thiết bị

TT	Nội dung yêu cầu	Tài liệu yêu cầu kèm theo E-HSDT
1	Dịch vụ đề xuất phải đáp ứng ở chế độ hỗ trợ toàn thời gian (24x7x365: 24 giờ trong ngày, 7 ngày trong tuần, tất cả các ngày trong năm).	Cam kết của Nhà thầu và tài liệu chứng minh
2	Thời hạn dịch vụ có hiệu lực: Tối thiểu là 1 năm (12 tháng hoặc đến hết ngày 31/12/2026) kể từ ngày kích hoạt dịch vụ (hoặc giấy phép, bản quyền)	Cam kết của Nhà thầu và tài liệu chứng minh
3	Trong thời gian thuê dịch vụ (giấy phép, bản quyền có hiệu lực): - Thời gian phản hồi thông tin kể từ khi nhận được các yêu cầu: + Đối với các sự cố quan trọng: tối đa là 1 giờ. + Đối với các sự cố không quan trọng: Trong ngày làm việc kế tiếp	Cam kết của Nhà thầu và tài liệu chứng minh

4.4.2 Hỗ trợ kỹ thuật, bảo trì, bảo hành, duy trì, giám sát hoạt động

TT	Nội dung yêu cầu	Yêu cầu tài liệu kèm theo E-HSDT
1	- Thời gian thực hiện cập nhật các phiên bản phần mềm (hệ điều hành, danh mục, dữ liệu bổ sung) mới nhất từ nhà sản xuất: Tối đa là 3 ngày làm việc kể từ thời điểm nhà sản xuất phát hành bản mới nhất; - Thời gian sửa chữa, khắc phục sự cố các lỗi, hư hỏng, hiệu chỉnh các sai lệch của thiết bị: tối đa 72 giờ kể từ khi nhận được yêu cầu (trừ trường hợp phải vận chuyển thiết bị tới địa điểm khác hoặc phải thực hiện thay thế vật tư thiết bị); - Thời gian thực hiện bảo trì, bảo dưỡng thiết bị: trong vòng 48 giờ, tối đa không quá 72 giờ kể từ thời điểm bắt đầu đến thời điểm hoàn thành toàn bộ công việc; - Thực hiện các biện pháp phòng ngừa chủ động, giảm thiểu tối đa các rủi ro, nguy cơ về lỗi, hỏng hóc, sự cố làm ảnh hưởng đến hoạt động của thiết bị: Tối thiểu 3 lần/năm - Thời gian thực hiện kiểm tra, giám sát, cung cấp thông tin về tình trạng hoạt động, tính năng vận hành, dự báo về các rủi ro, nguy cơ tiềm ẩn của thiết	Cam kết của Nhà thầu

TT	Nội dung yêu cầu	Yêu cầu tài liệu kèm theo E-HSDT
	bị: Tối đa 48 giờ kể từ khi nhận được yêu cầu - Thời gian hỗ trợ lắp đặt, cài đặt, thiết lập tham số, cập nhật phần mềm, dữ liệu khi có nhu cầu về chuyển đổi hệ thống, thay đổi vị trí, địa điểm vận hành; sửa đổi kiến trúc, giải pháp kỹ thuật, cách thức, phương thức vận hành kết nối: Tối đa là 72 giờ kể từ khi nhận được yêu cầu - Thời gian hỗ trợ kỹ thuật từ xa, tư vấn, trả lời các câu hỏi, giải đáp các thắc mắc, đáp ứng yêu cầu về đào tạo, hướng dẫn sử dụng; *+ Thời gian thực hiện các yêu cầu hỗ trợ kỹ thuật từ xa (giám sát, kiểm tra, hiệu chỉnh, thiết lập tham số, hướng dẫn người dùng…): tối đa 24 giờ kể từ khi nhận được yêu cầu.* *+ Thời gian trả lời câu hỏi, giải đáp các thắc mắc, yêu cầu tư vấn qua điện thoại, công cụ nhắn tin (chat) trực tuyến là tức thì; Qua thư điện tử (email). Công cụ hỗ trợ kết nối trực tuyến (như (teamviewer, ultraview…) là 30 phút, tối đa 8 giờ;* *+ Trường hợp không thể hỗ trợ kỹ thuật từ xa hoặc được chủ đầu tư yêu cầu, nhà thầu phải cử cán bộ có mặt tại địa điểm thực hiện để xử lý, giải quyết các lỗi, sự cố, hư hỏng và đề ra các biện pháp khắc phục trong vòng 12 giờ kể từ khi nhận được yêu cầu;* *+ Thời gian đào tạo hướng dẫn sử dụng, quản trị: tối đa là 24 giờ kể từ khi nhận được yêu cầu*	

5. Giải pháp và phương pháp luận

Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương này, gồm các phần như sau:

a. Giải pháp và phương pháp luận;

b. Kế hoạch triển khai thực hiện.

6. Các yêu cầu khác

Nhà thầu phải có đầy đủ các cam kết sau:

- Cam kết thực hiện hợp đồng và đáp ứng các yêu cầu về:

+ Thời hạn cung cấp, thực hiện, cho thuê dịch vụ theo quy định của E-HSMT;

+ Các quy chuẩn, tiêu chuẩn, định mức kỹ thuật có liên quan;

+ Yêu cầu về tích hợp, trao đổi dữ liệu với các hệ thống khác của Cục Quản lý và Phát triển thị trường trong nước;

+ Tuân thủ điều kiện vệ sinh môi trường, phòng cháy, chữa cháy, an toàn lao động.

+ *Các điều khoản của hợp đồng, điều kiện và phương thức thanh toán*

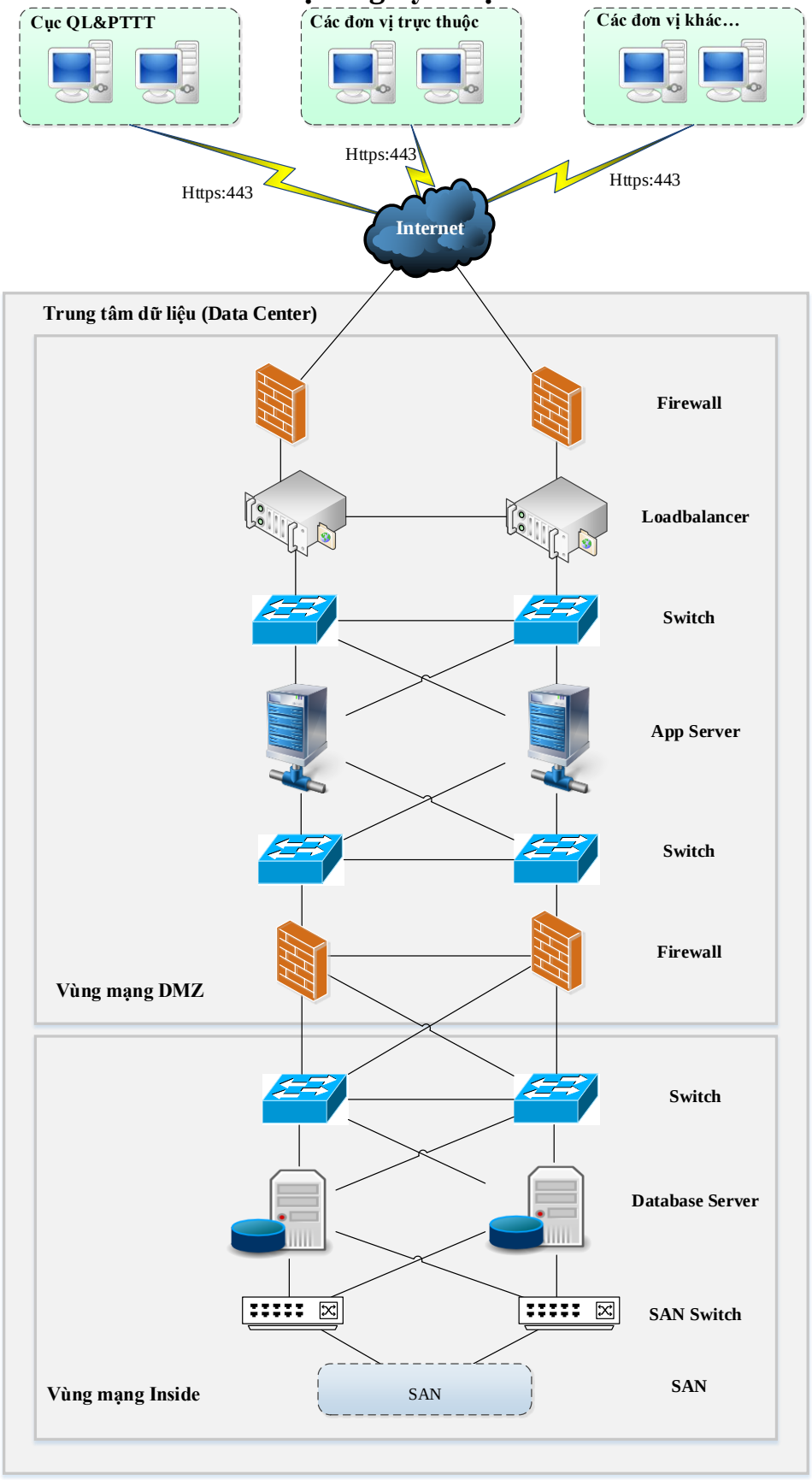
- Cam kết bảo mật thông tin, dữ liệu trong và cả sau khi hết thời gian cung cấp, thực hiện, cho thuê dịch vụ. Không tiết lộ cho bất kỳ bên thứ ba nào khi chưa có sự cho phép bằng văn bản của Cục Quản lý và Phát triển thị trường trong nước;

- Cam kết cung cấp, tuân thủ và đáp ứng yêu cầu về tài liệu gốc: Khi được Bên mời thầu yêu cầu, nhà thầu có nghĩa vụ cung cấp đầy đủ bản gốc các tài liệu cho Bên mời thầu để xác minh, đối chiếu nội dung với bản sao các tài liệu được công chứng/chứng thực đính kèm, kê khai trên hệ thống. Trường hợp Nhà thầu không cung cấp được bản gốc để phục vụ xác minh, đối chiếu thì Bên mời thầu sẽ không chấp nhận các tài liệu bản sao được công chứng/chứng thực mà Nhà thầu đã đính kèm, kê khai trên hệ thống

PHỤ LỤC: THÔNG TIN VỀ HẠ TẦNG CNTT VÀ THIẾT BỊ

1. Hạ tầng kỹ thuật

1.1. Mô hình kiến trúc hạ tầng kỹ thuật



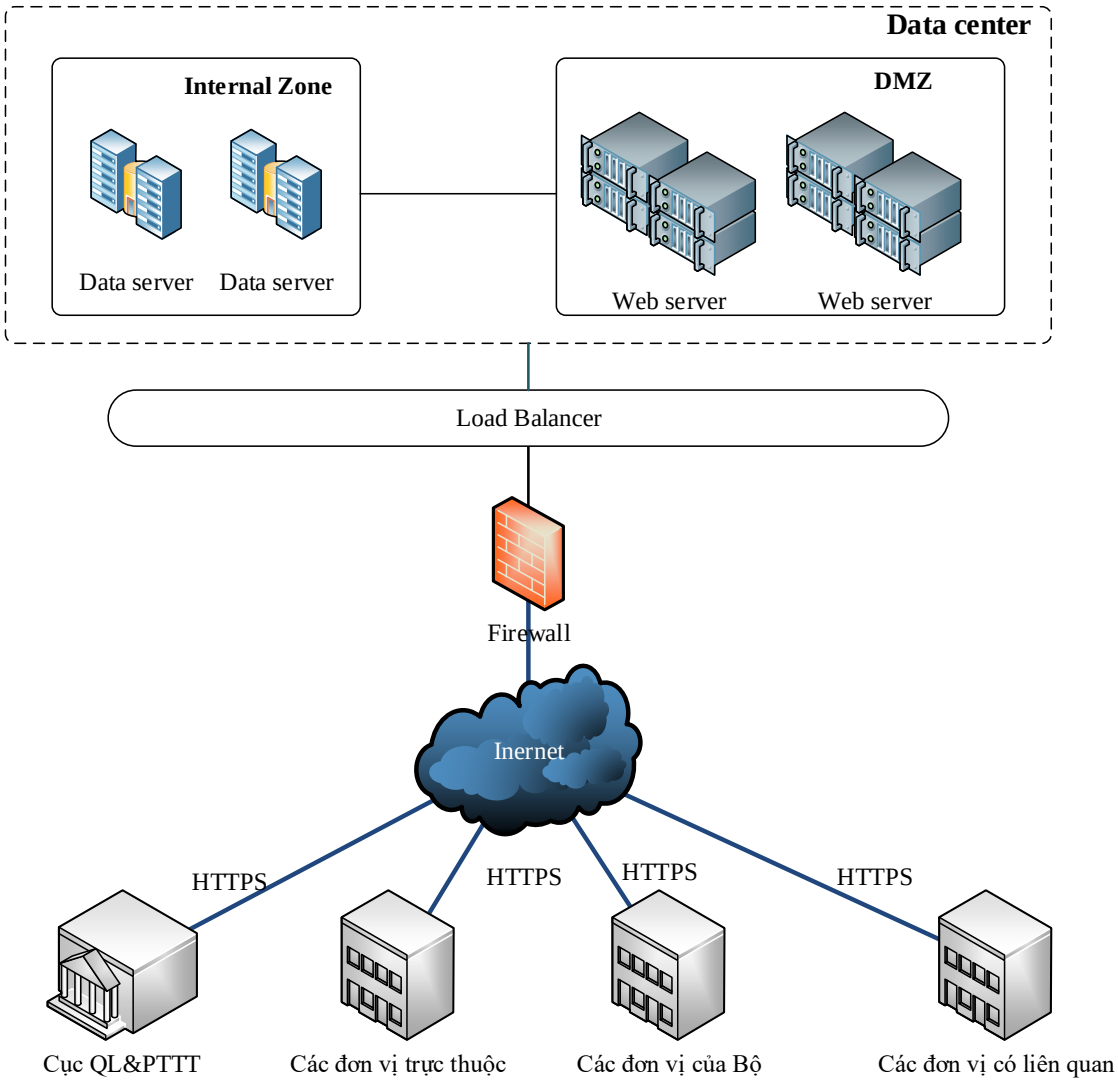
Hệ thống được cài đặt gồm các thành phần chính sau:

- Hệ thống máy chủ ứng dụng: Là hệ thống có nhiệm vụ xử lý các yêu cầu đến từ người dùng, thực hiện truy vấn các dữ liệu từ vùng máy chủ cơ sở dữ liệu (CSDL) và trả lại kết quả cho người dùng.

- Hệ thống máy chủ CSDL: Là hệ thống có nhiệm vụ tổ chức, lưu trữ dữ liệu của toàn hệ thống và xử lý các yêu cầu truy vấn, khai thác dữ liệu. Hệ thống máy chủ CSDL bao gồm 02 mày chủ chạy theo mô hình phân cụm (Clustering), 02 máy chủ vừa đóng vai trò phân tải (các yêu cầu xử lý của hệ thống sẽ được phân đều trên cả hai máy chủ), vừa đóng vai trò dự phòng (nếu một máy chủ CSDL gặp sự cố về phần cứng hoặc phần mềm dẫn đến không thể hoạt động được, thì các yêu cầu xử lý sẽ được chuyển sang máy chủ CSDL không có sự có để xử lý)

- Hệ thống cân bằng tải: Là hệ thống có nhiệm vụ phân chia các yêu cầu phục vụ từ người sử dụng đều cho các máy chủ thành viên trong cùng một vùng máy chủ ứng dụng.

1.2. Mô hình triển khai các ứng dụng



- Hệ thống được cài đặt, cấu hình và vận hành trên hệ thống máy chủ tại Trung tâm dữ liệu thuộc phạm vi gói thầu thuê dịch vụ hạ tầng kỹ thuật phục vụ vận hành các phần mềm ứng dụng.

- Triển khai tại Cục Quản lý và Phát triển thị trường trong nước- Bộ Công Thương, số 91, Đinh Tiên Hoàng - Hoàn Kiếm - Hà Nội.

- Hệ thống các phần mềm được triển khai theo phương thức làm việc trực tuyến (online):

+ Các đơn vị trực thuộc và các địa phương trên toàn quốc sẽ kết nối trực tiếp với máy chủ hệ thống đặt tại Trung tâm dữ liệu.

+ Trao đổi thông tin, dữ liệu theo các chuẩn về an toàn thông tin SSL v3.0, HTTPS. SSL là một tiêu chuẩn an ninh công nghệ toàn cầu tạo ra một liên kết giữa máy chủ web và trình duyệt. Liên kết này đảm bảo tất cả các dữ liệu trao đổi giữa máy chủ web và trình duyệt luôn được bảo mật và an toàn. SSL đảm bảo rằng dữ liệu truyền đi trong hệ thống được mang tính riêng tư, tách rời. HTTPS là phần mở rộng bảo mật của HTTP. Website được cài đặt chứng chỉ SSL có thể dùng giao thức HTTPS để thiết lập kênh kết nối an toàn tới máy chủ (server).

1.3. Địa chỉ lắp đặt thiết bị

Các thiết bị thuộc hạ tầng kỹ thuật được lắp đặt tại: Trung tâm dữ liệu VNPT tại Nam Thăng Long (Địa chỉ: Khu B2-1-6 Khu công nghiệp Nam Thăng Long - Hà Nội).

2. Thông tin về thiết bị (phạm vi danh mục thiết bị cần thực hiện dịch vụ)

2.1. Danh mục, ký mã hiệu, nhãn mác thiết bị

TT	Danh mục thiết bị	Ký mã hiệu, nhãn mác	SL	ĐVT
1	Thiết bị tường lửa	Fortigate FG-601E-BDL-950-36 kèm FN-TRAN-SFP+SR và SP-FG300E-PS, Fortinet	2	Chiếc
2	Thiết bị cân bằng tải ứng dụng	FortiADC FAD-400F-BDL-619-36 kèm SP-FAD400F-PS, Fortinet	2	Bộ

2.2. Thông số kỹ thuật của thiết bị

TT	Đặc tính, thông số kỹ thuật của thiết bị
1	**Thiết bị tường lửa**
	- Số cổng GE 1G RJ45 built-in: 8
	- Số cổng 1G SFP slot: 8
	- Số cổng 10 GE SFP+ slot: 2, Transceiver: 2 x SFP
	- Số cổng USB: 2
	- Số cổng quản trị: 2
	- Số cổng Console: 1

TT	Đặc tính, thông số kỹ thuật của thiết bị
	- Thông lượng tường lửa IPv4 (UDP 1518/64 byte): 36/27 Gbps
	- Thông lượng tưởng lửa IPv6 (UDP 1518/64 byte): 36/27 Gbps
	- Độ trễ tường lửa (64 byte, UDP): 1.54 µs
	- Thông lượng tường lửa (Gói trên giây): 40,5 Mpps
	- Các phiên đồng thời: 8.000.000
	- Các phiên mới/giây: 450.000
	- Chính sách tường lửa (Firewall Policies): 10.000
	- Thông lượng IPsec VPN (512 byte): 20 Gbps
	- Thông lượng SSL-VPN: 7 Gbps
	- Số người dùng SSL-VPN đồng thời: 10.000
	- Thông lượng SSL Inspection (với IPS, avg HTTPS): 8 Gbps
	- SSL Inspection CPS (with IPS, avg HTTPS): 5.500
	- Phiên kiểm tra đồng thời SSL (with IPS, avg HTTPS): 800.000
	- Thông lượng IPS (Enterprise Mix): 10 Gbps
	- Băng thông Next Gen Firewall: 9,5 Gbps
	- Thông lượng Threat Protection (Firewall, IPS, Application control, Malware Protection enabled on Enterprise Traffic Mix): 7 Gbps
	- Dung lượng lưu trữ: 2 x 240 GB SSD
	- Bản quyền phần mềm cho các tính năng và dịch vụ bảo hành phần cứng, hỗ trợ kỹ thuật chính hãng: Thiết bị có đầy đủ bản quyền sử dụng các tính năng Antivirus (Malware Protection, Cloud Sandboxing), NGFW (IPS và Application Control), Web Filtering, Antispam, thời hạn 03 năm
	- Kiến trúc phần cứng: + Kiến trúc tăng tốc phần cứng, sử dụng Security Processing Unit (SPU) xử lý cộng tác với CPU: • Chip tăng tốc xử lý chuyên biệt cho tính năng bảo mật sử dụng kỹ thuật so khớp signature; tối ưu khả năng mã hoá/giải mã dữ liệu. • Chip tăng tốc xử lý chuyên biệt cho dữ liệu Firewall IPv4, IPv6, SCTP và Multicast, VPN và IP Tunnel. - Kiến trúc xử lý song song Parallel Path Processing, dùng cấu hình chính sách của tường lửa để lựa chọn từ nhóm các tùy chọn song song nhằm quyết định hướng xử lý tối ưu cho gói tin dữ liệu.
	- Tính năng SD-WAN: + Tính năng Software-defined WAN được phát triển và xây dựng từ cùng nhà sản xuất nhằm đảm bảo mức độ tương thích cao nhất + Cân bằng tải đường WAN theo các thuật toán dựa vào trọng số (weighted) sau: Volume, Session, Source-Destination IP, Source IP và spillover. + Kiểm tra kết nối WAN theo SLAs: • Ping hoặc HTTP • Giám sát dựa theo các thông số Latency, Jitter và Packet Loss • Có khả năng cấu hình ngưỡng theo Interval, Failure và Fail-back + Chính sách đa đường thông minh được định nghĩa bởi:

TT	Đặc tính, thông số kỹ thuật của thiết bị
	• Địa chỉ nguồn và/hoặc nhóm người dùng • Địa chỉ đích và và/hoặc lựa chọn hơn 3.000 ứng dụng • Lựa chọn đường đi (path) dựa theo chất lượng hoặc SLAs được định nghĩa
	- Tính năng VPN: + Hỗ trợ tính năng IPSec Aggregate tunnels: • Thiết lập dự phòng và cân bằng tải dữ liệu. • Hỗ trợ cân bằng tải trên từng gói tin (Per-packet) theo các thuật toán: IP Addresses, L4 information và (weighted) round-robin. + Auto Discovery VPN (ADVPN): Tự động thiết lập Tunnel kết nối (đường tắt - shortcuts) giữa các Spoke trong kiến trúc Hub và Spoke. + UDP Hole Puching hỗ trợ thiết lập kết nối shortcut giữa các Spoke nằm sau lớp NAT + Hỗ trợ triển khai theo các chế độ: Gateway-to-Gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN terminate in transparent mode
	- Khả năng thiết lập chính sách theo từng loại đối tượng: Thiết bị có khả năng thiết lập các chính sách truy cập theo người dùng (Identity-based Policy), theo loại thiết bị gia nhập mạng (device-based Policy)
	- Khả năng phòng chống tấn công, chặn Web, ứng dụng: + Hỗ trợ chế độ kiểm tra lọc Web: Proxy-based, flow-based và DNS + Cơ chế lọc Web tự động với cơ sở dữ liệu phân loại web theo thời gian thực: Hỗ trợ tìm kiếm an toàn (Safe Search), tự động thêm vào tham số tìm kiếm an toàn cho các nội dung truy vấn: Hỗ trợ Google, Yahoo!, Bing and Yandex, Youtube Education Filter. + IPS Engine: Phát hiện giao thức bất thường, ngưỡng bất thường, signature tự định nghĩa. + Thiết bị có khả năng chống tấn công DOS cơ bản với các tính năng: TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding (source/destination) + Ngăn chặn IP Botnet Server với Cơ sở dữ liệu IP Reputation
	+ Lọc virus thông qua các giao thức và dạng file sau: • Hỗ trợ HTTP, FTP, IMAP, POP3, SMTP, NNTP, MAPI, CIFS và SSH • Phát hiện dữ liệu mã hóa với SSL Inspection • Hỗ trợ phát hiện Grayware và Mobile Malware + Cho phép Content Disarm and Reconstruction: • AV Engine loại bỏ nội dung động theo thời gian thực trước khi gửi cho người dùng • Gửi tập tin ban đầu tới Sandbox để phân tích, cách ly hoặc loại bỏ + Phát hiện ứng dụng trong nhiều dạng: Business, Cloud IT, Collaboration, Email, Game, General Interest, Mobile, Network Service, P2P, Proxy, Remote Access, Social Media, Storage/Backup, Update, Video/Audio, VoIP, Web Chat

TT	Đặc tính, thông số kỹ thuật của thiết bị
	- Hỗ trợ các giao thức định tuyến: Hỗ trợ các giao thức định tuyến tĩnh, Policy Based Routing và định tuyến động như RIP, OSPF
	- Hỗ trợ chứng thực: + Hỗ trợ chứng thực với các máy chủ AD, LDAP, RADIUS + Hỗ trợ chức năng chứng thực 2-Factor với token, cho phép chứng thực với sản phẩm token vật lý, token mềm của cùng hãng sản xuất
	- Hỗ trợ chế độ giám sát: Hỗ trợ chế độ giám sát Threat Map: hiển thị phân bổ các hiểm họa an ninh Thông tin toàn cầu; Device Topology: Hiển thị mô hình kết nối luận lý giữa các thiết bị trong mạng
	- Hỗ trợ chức năng tự động hoá: Quản trị viên lập trình sẵn hành vi phản ứng khi có các sự cố (incident/event)
	- Hỗ trợ cơ chế sẵn sàng cao (HA): Active - Active, Active - Passive, Clustering
	- Hỗ trợ quản trị bằng Web GUI, CLI, SNMP, hoặc thiết bị quản trị tập trung
	- Nguồn điện: 02 nguồn
	- Bảo hành: Bảo hành và gói dịch vụ hỗ trợ kỹ thuật nâng cao chính hãng, đáp ứng SLA 24x7
2	**Thiết bị cân bằng tải ứng dụng: FortiADC FAD-400F-BDL-619-36 kèm SP-FAD400F-PS, Fortinet**
	- Năng lực xử lý thông lượng L4/L7: 15 Gbps/12 Gbps
	- L4 CPS: 400.000
	- Năng lực xử lý số lượng kết nối đồng thời L4 (Concurrent Connection): 12.000.000
	- Năng lực xử lý SSL CPS/TPS (2K keys): 15.000
	- Năng lực xử lý mã hóa SSL: 6 Gbps
	- Năng lực xử lý nén trên phần cứng chuyên dụng (Hardware Compression Throughput): 10 Gbps
	- Dung lượng bộ nhớ (RAM): 32 GB
	- Số lượng cổng mạng: 2x 10 GE SFP+, 4x GE SFP, 4x GE RJ45
	- Dung lượng ổ cứng: 120 GB SSD
	- Nguồn điện: 2 nguồn
	- Hỗ trợ ảo hóa thiết bị (Virtual Domains): 20
	- Tính năng cân bằng tải + Tính sẵn sàng ứng dụng: • Trên Virtual service/Server có thể định nghĩa: Giữ phiên làm việc theo persistence, thuật toán cân bằng tải, và pool members • Hỗ trợ chính sách định tuyến ứng dụng mức Layer 4/7 • Hỗ trợ tính năng giữ phiên làm việc: Persistence ở mức Layer 4/7 • Có khả năng giám sát tình trạng hoạt động của ứng dụng dựa trên tính năng tùy biến bằng Script
	+ Tính năng cân bằng tải:

TT	Đặc tính, thông số kỹ thuật của thiết bị
	• Hỗ trợ cân bằng tải các giao thức hoặc ứng dụng: TCP, UDP, IP, DNS, HTTP, HTTPS, HTTP 2.0 GW, FTP, SIP, RDP, RADIUS, MySQL, MSSQL, RTMP, RTSP, và các ứng dụng phổ biến khác • Hỗ trợ L7 content switching and rewriting • Hỗ trợ URL Redirect, HTTP request/response rewrite (includes HTTP body) • Hỗ trợ cân bằng tải Layer 7 DNS, bảo mật và caching
	+ Tính năng cân bằng tải cho đường truyền • Hỗ trợ tính năng Cân bằng tải đường truyền cả chiều Inbound và Outbound • Hỗ trợ tính năng Route và NAT • Hỗ trợ giám sát kiểm tra (health check) chất lượng đường truyền
	- Tính năng tăng tốc ứng dụng: + Tính năng Offloading và tăng tốc SSL: • Hỗ trợ tính năng Offloads HTTPS and TCPS • Có khả năng quản lý đầy đủ các Certificate • Có tính năng HTTP/S Mirroring để phân tích báo cáo lưu lượng • Hỗ trợ TLS 1.3 + Tính năng tối ưu HTTP and TCP: • Có khả năng tăng tốc và giảm tải cho việc xử lý TCP • Connection pooling and multiplexing for HTTP and HTTPS • Hỗ trợ tính năng tăng tốc HTTP để tối ưu máy chủ Web • Hỗ trợ TCP buffering • Hỗ trợ nén và giải nén HTTP • Hỗ trợ HTTP Caching (static and dynamic objects) • Hỗ trợ tính năng Quality of Service (QoS) + Tính năng Authentication Offloading: Hỗ trợ Authentication Offloading cho các phương thức xác thực như: Local, LDAP, RADIUS, Kerberos, SAML 2.0 (SP and Idp), NTLM, Two-Factor Authentication - Token/Token Cloud and Google Authentication
	- Tính năng quản trị + Hỗ trợ cấu hình và giám sát thông qua CLI Interface + Hỗ trợ quản trị thông qua Web UI + Có khả năng phân quyền cho người quản trị (Role-based administration) + Có khả năng tạo báo cáo + Hỗ trợ REST API + Có khả năng phân tích dữ liệu theo thời gian thực
	- Tính năng bảo mật + Hỗ trợ IP Reputation Service + Có tính năng Web Application Firewall: Web Attack Signatures; XML/JSON Validation; SQLi/XSS Injection Detection; Bot Detection; URL Protection, File Restriction

TT	Đặc tính, thông số kỹ thuật của thiết bị
	- Thiết bị có bản quyền cho gói hỗ trợ dịch vụ nâng cao đáp ứng 24/7 (IPS, WAF Security Service, IP Reputation, Cloud Sandbox and Credential Stuffing Defense Service)
	- Bảo hành: Bản quyền phần mềm cho các tính năng, bảo hành và gói dịch vụ hỗ trợ kỹ thuật nâng cao chính hãng, đáp ứng SLA 24x7