Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Giới thiệu chung về dự án, gói thầu:

- Tên gói thầu: DV-01 "Cung cấp dịch vụ gia hạn thiết bị và phần mềm bảo mật, phần mềm diệt virus".

- Địa điểm thực hiện: Số 7 Phan Đình Phùng, phường Hoàn Kiếm, Tp Hà Nội.

- Nội dung chính của gói thầu: Cung cấp dịch vụ gia hạn thiết bị và phần mềm bảo mật, phần mềm diệt virus.

- Thời gian thực hiện gói thầu: 60 ngày.

2. Mục tiêu công việc:

Cung cấp dịch vụ gia hạn thiết bị và phần mềm bảo mật, phần mềm diệt virus cho Báo Quân đội nhân dân phải đảm bảo chất lượng, yêu cầu kỹ thuật và tiến độ hoàn thành dịch vụ.

3. Yêu cầu kỹ thuật của gói thầu:

3.1. Yêu cầu chung :

- Dịch vụ cung cấp cho gói thầu phải đồng bộ, có nguồn gốc từ chính hãng.

- Dịch vụ phải được cài đặt, vận hành hoàn toàn tương thích trên các trang thiết bị hiện có của Báo Quân đội nhân dân, không gây ảnh hưởng và gián đoạn vận hành an toàn của toàn bộ hệ thống.

3.2. Yêu cầu kỹ thuật cụ thể

Tóm tắt yêu cầu của dịch vụ phải đáp ứng các thông số kỹ thuật và tiêu chuẩn sau đây:

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn(*)
1.	- Gia hạn dịch vụ bảo hành, bảo trì và hỗ trợ kỹ thuật thiết bị tường lửa chuyên dụng bảo vệ ứng dụng web - Imperva X2020 (12 tháng). - Gia hạn dịch vụ bảo hành, bảo trì và hỗ trợ kỹ thuật thiết bị tường lửa chuyên dụng bảo vệ ứng	*a. <u>Yêu cầu chung:</u>* - Gia hạn bảo hành thiết bị tường lửa Imperva từ chính hãng sản xuất hoặc nhà cung cấp chính thức được ủy quyền. - Cập nhật và gia hạn bản quyền phần mềm thiết bị tường lửa Imperva từ chính hãng sản xuất hoặc nhà cung cấp chính thức được ủy quyền. - Yêu cầu về cung cấp bản quyền và dịch vụ bảo hành: 12 tháng, có hỗ trợ kỹ thuật 24/7 trong suốt thời hạn sử dụng. - Thiết bị sau khi được cập nhật phần mềm và gia hạn bản quyền có thể tiếp tục sử dụng ngay, không yêu cầu cài đặt hoặc hiệu chỉnh lại các tham số hệ thống. *b. <u>Yêu cầu chi tiết:</u>* Sau khi gia hạn bản quyền sử dụng thiết bị tường lửa Imperva

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn(*)
	dụng web - Imperva X2520 (12 tháng). - Gia hạn bản quyền phần mềm Client Reputation Services for 2000 Series, Enterprise Edition, Annual Subscription (Cập nhật cho các thiết bị Imperva) (12 tháng).	phải đảm bảo: - Về chính sách sử dụng: + Được cập nhật các tính năng mới: khi Hãng hoàn thiện và cập nhật một tính năng bảo vệ mới thì thiết bị sẽ được cập nhật bổ sung tính năng đó ngay sau khi Hãng công bố và cho phép cập nhật. + Cập nhật được các hình thức tấn công mới vào ứng dụng web: ngay khi một hình thức tấn công mới vào ứng dụng web được phát hiện và ngăn chặn, thiết bị được tự động cập nhật hình thức tấn công đó. - Về tính năng thiết bị: ✓ Khả năng ngăn chặn được các hình thức tấn công đã được nêu OWASP Top 10: + Injection + Cross-Site Scripting (XSS) + Broken Authentication and Session Management + Insecure Direct Object References + Cross-Site Request Forgery (CSRF) + Security Misconfiguration + Insecure Cryptographic Storage + Failure to Restrict URL Access + Insufficient Transport Layer Protection + Unvalidated Redirects and Forwards ✓ Cung cấp dịch vụ chống tấn công dựa theo Reputation-based (Reputation-based Web security): + Cung cấp Reputation-Based Security nhằm ngăn chặn các tấn công tự động và từ nguồn không tin cậy bao gồm Malicious IP, Anonymous Proxies,The Onion Router (TOR) Networks, Phishing URLs. + Hỗ trợ IP Geolocation, chặn IP theo vị trí địa lý cụ thể, cho phép giám sát và chặn truy cập từ các quốc gia không mong muốn. + Hỗ trợ "Community Defense", thu thập các thông tin tấn công từ cộng đồng người dùng đã triển khai cùng sản phẩm của hãng sản xuất và chuyển thành mẫu tấn công, chính sách,..để bảo vệ hệ thống. ✓ Chống tấn công Bot và tấn công tự động: + Cung cấp công nghệ Anti-automation để phát hiện các client tự động, bot, cripts based trên Web browser + Cung cấp chính sách an ninh site scraping, Application DDoS,

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn(*)
		Google hacking ✓ Universal User Tracking: Tự động truy vết được user của ứng dụng Web. ✓ Bảo vệ ứng dụng: + Tự động học ứng dụng và hành vi người dùng. Tự động cập nhật các thay đổi hợp lệ của ứng dụng và đưa vào hồ sơ học ứng dụng + Có khả năng chống lại các tấn công đã biết nhằm vào các điểm yếu của máy chủ Web, máy chủ ứng dụng và hệ điều hành. Chống sâu (worm) đã biết và zero-day để bảo vệ nền tảng (flatform) + Hỗ trợ tối thiểu 8000 mẫu tấn công (Signature) + Có khả năng Kiểm tra tuân thủ giao thức HTTP để đảm bảo rằng các truy cập Web tuân theo tiêu chuẩn RFC nhằm phát hiện ra các bất thường trong địa chỉ URL và các giao thức ✓ Các phương pháp bảo vệ cookies: + Cookie injection, cookie poisoning + Stateful firewall, DoS prevention ✓ Cung cấp correlation engine: Có khả năng phân tích tương quan nhiều sự kiện để cho phép xử lý các hành vi/vi phạm đáng ngờ bằng việc đánh giá các sự kiện qua khoảng thời gian và qua nhiều lớp phát hiện (malicious encoding, HTTP protocol violations, application proile violations, data leak prevention, signatures, Web worms) ✓ Có khả năng "Vá ảo" (Virtual Patch) qua khả năng tích hợp với các giải pháp quét điểm yếu: + Có khả năng tích hợp với các giải pháp quét điểm yếu của hãng thứ ba, bao gồm WhiteHat, IBM, Cenzic, NT OBJECTives, HP, Qualys, Beyond Security, Acunetix, Denim Group + Cung cấp bản vá ảo để bảo vệ các điểm yếu được phát hiện. ✓ Hỗ trợ mở rộng khả năng chống gian lận trong giao dịch trực tuyến ứng dụng (Web Fraud Prevention): Hỗ trợ tùy chọn mở rộng tích hợp với các giải pháp chống gian lận trong giao dịch trực tuyến (Web Fraud Prevention) của hãng thứ ba: ThreatMetrix, iovation, Trusteer. ✓ Tìm phát hiện máy chủ ứng dụng Web: tìm phát hiện các máy chủ ứng dụng Web với các dữ liệu nhạy cảm. ✓ Logging/Monitoring: + SNMP, Syslog, Email + Integrated graphical reporting (HTML, PDF, CSV formats)

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn(*)
		+ Real-time dashboard
2.	Gia hạn bản quyền phần mềm quản trị tập trung các tường lửa bảo vệ ứng dụng web - VM150 (12 tháng)	*a. <u>Yêu cầu chung</u>:* - Cập nhật và gia hạn bản quyền hệ thống phần mềm quản trị tập trung các tường lửa bảo vệ ứng dụng web (VM150) từ chính hãng sản xuất hoặc nhà cung cấp chính thức được ủy quyền. - Yêu cầu về cung cấp bản quyền phần mềm: tối thiểu 12 tháng trở lên, có hỗ trợ kỹ thuật 24/7 trong suốt thời hạn bản quyền. - Hệ thống phần mềm sau khi gia hạn tiếp tục sử dụng ngay, không yêu cầu cài đặt và hiệu chỉnh lại các tham số của hệ thống. *b. <u>Yêu cầu chi tiết</u>:* Hệ thống phần mềm sau khi cập nhật và gia hạn phải đảm bảo vận hành đầy đủ các tính năng cơ bản sau: + Cho phép triển khai dưới dạng thiết bị vật lý chuyên biệt hoặc triển khai trên các nền tảng ảo hoá như VMware Hypervisor hay Hyper-V Hypervisor. + Cung cấp giao diện thực hiện auditing, reporting và lưu log các sản phẩm SecureShphere. + Thể hiện trạng thái về bảo mật và giám sát các incident theo thời gian thực thông qua live security dashboard. + Cung cấp giao diện điều tra và phân tích các hoạt động của người dùng. + Giám sát toàn bộ các thông số về trạng thái hoạt động của hệ thống trên một giao diện. + Quản lý và phân phối các chính sách cho các thiết bị được quản lý trên toàn bộ các thiết bị WAF/DBFW của Imperva. + Cung cấp kiểm soát truy cập quản trị phân quyền. Giám sát được hoạt động và trạng thái của toàn bộ thiết bị cũng như các hoạt động trong môi trường bảo mật.
3.	Gia hạn dịch vụ hỗ trợ kỹ thuật và bảo hành thiết bị Citrix ADC MPX 5905 Advanced Edition (12 tháng).	*a. <u>Yêu cầu chung</u>:* - Gia hạn bảo hành thiết bị cân bằng tải Citrix từ chính hãng sản xuất hoặc nhà cung cấp chính thức được ủy quyền. - Cập nhật và gia hạn bản quyền phần mềm thiết bị cân bằng tải Citrix từ chính hãng sản xuất hoặc nhà cung cấp chính thức được ủy quyền. - Yêu cầu về cung cấp bản quyền và bảo hành: tối thiểu 12 tháng trở lên, có hỗ trợ kỹ thuật 24/7 trong suốt thời hạn sử dụng. - Thiết bị sau khi được cập nhật phần mềm và gia hạn bản

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn(*)
		quyền có thể tiếp tục sử dụng ngay, không yêu cầu cài đặt hoặc hiệu chỉnh lại các tham số hệ thống. *b. <u>Yêu cầu chi tiết:</u>* - Sau khi gia hạn bản quyền sử dụng thiết bị cân bằng tải Citrix phải đảm bảo: - Về chính sách sử dụng: + Duy trì dịch vụ hỗ trợ từ Hãng khi có sự cố xảy ra + Cập nhật các tính năng mới khi hãng đưa ra các bản cập nhật. + Thay thế thiết bị mới khi có lỗi với phần cứng. - Về tính năng thiết bị: ✓ Cân bằng tải lớp 4: + Giao thức hỗ trợ: TCP, UDP, FTP, HTTP, HTTPS, DNS (TCP and UDP), SIP (over UDP), RTSP, RADIUS, SQL, RDP. + Thuật toán cân bằng tải thông minh: Round Robin, Least Packets, Least Bandwidth, Least Connections, Response Time, Hashing (URL, Domain, Source IP, Destination IP, and CustomID), SNMP-provided metric, Server Application State Protocol (SASP). + Hỗ trợ các cơ chế giữ phiên làm việc: Source IP, cookie,server, group, SSL session, SIP CALLID,Token-based, JSESSIONID. + Hỗ trợ cơ chế kiểm tra trạng thái máy chủ: Ping, TCP, URL, ECV, scriptable health checks, Dynamic Server Response Time. ✓ Chuyển mạch nội dung lớp 7: Các chính sách: URL, URL Query, URL Wildcard, Domain, Source/Destination IP, HTTP Header, Custom, HTTP and TCP Payload Values, UDP. ✓ Cân bằng tải cơ sở dữ liệu: Hỗ trợ Microsoft SQL Server và MySQL; Thuật toán switching bao gồm các tham số truy vấn SQL như tên cơ sở dữ liệu, người dùng và tham số câu lệnh. ✓ Cân bằng tải đường truyền: Cân bằng tải lưu lượng inbound và outbound qua nhiều kết nối Internet. ✓ Khả năng chống DDoS lớp 4; Hỗ trợ kiểm soát truy cập lớp 3,4 (access list); Có khả năng lọc nội dung lớp 7; Có khả năng sửa đổi địa chỉ URL. ✓ Tăng tốc ứng dụng: tối ưu hóa TCP. + Multiplexing, Buffering, ConnectionKeep-alive, Windows

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn(*)
		Scaling, Selective Acknowledgement, Fast Ramp. + Tăng tốc và giảm tải SSL. + Chính sách định nghĩa dựa trên giá trị HTTP header và body.
4.	Gia hạn bản quyền phần mềm thiết bị tường lửa lớp mạng Sophos XGS (12 tháng)	*a. Yêu cầu chung:* - Cập nhật và gia hạn bản quyền phần mềm thiết bị tường lửa lớp mạng Sophos XSG từ chính hãng sản xuất hoặc nhà cung cấp chính thức được ủy quyền. - Yêu cầu về cung cấp bản quyền và bảo hành: tối thiểu 12 tháng trở lên, có hỗ trợ kỹ thuật 24/7 trong suốt thời hạn sử dụng. - Thiết bị sau khi được cập nhật phần mềm và gia hạn bản quyền có thể tiếp tục sử dụng ngay, không yêu cầu cài đặt hoặc hiệu chỉnh lại các tham số hệ thống. *b. Yêu cầu chi tiết:* - Cập nhật và gia hạn bản quyền cho phép thiết bị cập nhật phiên bản mới nhất của hệ điều hành và các mẫu tấn công, virus giúp bảo vệ hệ thống mạng tốt hơn. - Mở khóa các tính năng Firewall cao cấp bị đóng do hết hạn bản quyền. - Gia hạn bản quyền sẽ mở các tính năng bảo vệ cao cấp: Network Security, Mail Security, Web Security, Web Application Security, Wireless Security. - Đảm bảo có các tính năng sau khi gia hạn bản quyền: + **Network Protection** ▪ Công cụ IPS thế hệ mới với hiệu năng cao, sử dụng kỹ thuật kiểm tra sâu gói tin (Deep Packet Inspection), cho phép áp dụng các mẫu IPS chọn lọc theo từng quy tắc firewall nhằm đạt hiệu năng và mức bảo vệ tối ưu. ▪ Hàng nghìn chữ ký (signature) phát hiện tấn công ▪ Hỗ trợ tạo và sử dụng chữ ký IPS tùy chỉnh + **Advanced Threat Protection** ▪ Active Threat Response tự động giám sát và chặn các mối đe dọa APT cùng các nguy cơ khác được nhận diện thông qua nguồn dữ liệu đe dọa, cung cấp khả năng bảo vệ nâng cao trước bot và các tác nhân tấn công đang hoạt động khi chúng cố gắng kết nối tới các điểm đến độc hại, bằng cách sử dụng cơ chế phát hiện đa lớp gồm DNS, AFC và hệ thống firewall. + **Web Protection** ▪ Cơ sở dữ liệu lọc URL với hàng triệu website được phân

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn(*)
		loại thành 92 danh mục ▪ Application Control: Kiểm soát ứng dụng dựa trên chữ ký (signature-based), với các mẫu nhận diện cho hàng nghìn ứng dụng. ▪ Công cụ phát hiện mã độc độc lập thứ hai (Avira) để thực hiện dual scanning. ▪ Bảo vệ nâng cao chống mã độc trên web với công nghệ giả lập JavaScript. ▪ Chính sách thời gian truy cập theo từng người dùng hoặc nhóm. + **Email Protection** ▪ Ngăn chặn spam mail và các loại mã độc lây nhiễm qua Email. ▪ Công cụ phát hiện mã độc độc lập thứ hai (Avira) để thực hiện dual scanning. ▪ Phát hiện link URL lừa đảo đính kèm ở trong email + **VPN** ▪ Hỗ trợ các giao thức VPN: SSL, IPsec, 256 bit AES/3DES, PFS, RSA, X509. + **Web Application Firewall Protection** Bảo vệ hệ thống Web server thông qua các tính năng: Reverse proxy, URL hardenling, Form hardenling, SQL Injection, XSS, Dual Anti-Virus.
5.	- Gia hạn bản quyền phần mềm bảo mật Rapid7 Nexpose (12 tháng) - Gia hạn bản quyền phần mềm bảo mật Rapid7 Metasploit (12 tháng)	*a. <u>Yêu cầu chung:</u>* - Cập nhật và gia hạn bản quyền phần mềm bảo mật Rapid7 Nexpose và Rapid7 Metasploit từ chính hãng sản xuất hoặc nhà cung cấp chính thức được ủy quyền. - Yêu cầu về cung cấp bản quyền phần mềm: tối thiểu 12 tháng trở lên, có hỗ trợ kỹ thuật 24/7 trong suốt thời hạn bản quyền. - Các phần mềm sau khi gia hạn tiếp tục sử dụng ngay, không yêu cầu cài đặt và hiệu chỉnh lại các tham số của hệ thống. *b. <u>Yêu cầu chi tiết:</u>* - Cập nhật phần mềm và gia hạn bản quyền sử dụng phần mềm cho phép phần mềm thực hiện các chức năng sau: ▪ Cập nhật: Cập nhật dữ liệu mới nhất về các lỗ hổng bảo mật, cập nhật mới nhất về các phương thức tấn công mạng cho phần mềm. ▪ Tính năng dò quét hỗ trợ: có khả năng dò quét phát hiện hơn 35.000 lỗ hổng bảo mật và với hơn 100.000 cách kiểm tra khác nhau. ▪ Hỗ trợ phát hiện lỗ hổng của: Network, OS, Desktop

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn(*)
		Application, Web Application, Database Vulnerability. ▪ Dò quét cơ sở dữ liệu cho phép cấu hình để dò quét cho: MS SQL/Server versions 6, 7, 2000, 2005, 2008, Oracle versions 6 through 10, Sybase Adaptive Server Enterprise (ASE) versions 9, 10 and 11, DB2, AS/400,PostgreSQL versions 6, 7, 8, MySQL. ▪ Dưa thông tin lỗ hổng bảo mật có thêm các loại Malware hay Exploit có thể tấn công vào lỗ hổng đã được dò quét trong hệ thống. ▪ Cho phép loại bỏ các nguy cơ nhanh hơn với các ưu tiên được đưa ra dựa trên các ảnh hưởng có thể xảy ra. ▪ Kết hợp với công cụ khai thác: chương trình dò quét cho phép kết hợp với công cụ tấn công khai thác lỗ hổng bảo mật, nhằm mục đích kiểm tra lại ảnh hưởng khi lỗ hổng bảo mật của hệ thống mạng bị tấn công. ▪ Cập nhật lỗ hổng bảo mật: chương trình cho phép thường xuyên cập nhật các lỗ hổng bảo mật mới. ▪ Thực hiện vá lỗ hổng: cho phép vá lỗ hổng được thông báo "Tuesday vulnerability", thực hiện vá và kiểm tra lỗ hổng bảo mật ở mức độ hệ điều hành và hỗ trợ các hệ điều hành sau: Microsoft Windows, Red Hat, CentOS, Solaris, Vmware. ▪ Cho phép thiết lập giới hạn: chương trình dò quét cho phép tạo ra các mẫu (temp) nhằm giới hạn các mục tiêu dò quét. ▪ Cảnh báo trong quá trình dò quét: chương trình dò quét có tính năng cảnh báo cho người quản trị khi phát hiện một lỗ hổng bảo mật nào đó do người quản trị thiết lập. ▪ Kết hợp với các chương trình khác: chương trình cho phép kết hợp với các chương trình từ hãng thứ ba dựa trên XML-Base Open API. Chương trình dò quét cho phép làm việc được với một số ứng dụng bảo mật khác như hệ thống: IDS/IPS, SIEM/Log Mgmt, Pen Testing & Exploit Analysis. ▪ Báo cáo: chương trình có thể đưa ra báo cáo đầy đủ và chi tiết về hiện trạng lỗ hổng bảo mật của hệ thống mạng. ▪ Tính năng hỗ trợ cao cấp: ✓ Dò quét lỗ hổng bảo mật của ứng dụng web: chương trình dò quét có khả năng dò quét phát hiện lỗ hổng bảo mật của ứng dụng Web, phát hiện các lỗ hổng bảo mật ứng dụng web như: SQL Injection, XSS, và OWASP Top 10 Web Application Security Risks AJAX, ASP.NET 2.0, and Flash và Web Application.

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn(*)
		✓ Thiết lập tùy biến các mẫu dò quét: chương trình cho phép thiết lập, tùy chỉnh thay đổi các mẫu dò quét. ✓ Các thiết lập cơ bản về tài nguyên: chương trình cho phép tạo ra các nhóm tài nguyên phù hợp với các vùng mạng để người quản trị dễ dàng dò quét và phân vùng tài nguyên. ✓ Tùy biến báo cáo: chương trình dò quét cho phép tùy biến nhiều kiểu về nội dung và cách hiển thị cho phép dễ dàng tạo báo cáo phù hợp với những yêu cầu cụ thể của người quản trị. Chương trình cho phép xuất ra nhiều dạng file báo cáo khác nhau. ✓ Cho phép tùy biến CSV Export: cho phép tùy chỉnh dạng CSV khi xuất file. ✓ Báo cáo theo mẫu PCI: cho phép xuất báo cáo theo mẫu PCI. ▪ Tính năng cụ thể sau khi cập nhật phần mềm và gia hạn bản quyền sử dụng phần mềm: ✓ Quản trị: - Sử dụng quản trị qua Web (HTTPS), cho phép tạo phân quyền truy cập cho các user để quản trị dễ dàng và nâng cao tính bảo mật. - Thông tin người dùng có thể kết hợp với các dịch vụ quản lý người dùng như Active Directory, LDAP. ✓ Khám phá hệ thống mạng: - Hỗ trợ hai dạng khám phá hệ thống mạng: Dynamic và Static Sites. - Cho phép thiết lập thông tin đăng nhập (UserID và Password) để scan hệ thống mạng. Hỗ trợ các protocol: CVS, Sybase, DB2, SSH, Oracle, Telnet, CIFS, FTP, POP, HTTP, SNMP, SQL/Server, SMTP - Hỗ trợ phát hiện mạng bằng phương thức Dynamic cho cả các tài nguyên ảo hóa. ✓ Hình thức scan: hỗ trợ đặt lịch tự động scan hay scan thực hiện bởi người quản trị. Trong lúc scan có thể tạm dừng và xem thông tin kết quả. ✓ Quản lý tài nguyên: cho phép quản lý tài nguyên dựa trên các vùng tài nguyên (Sites). Hỗ trợ quản lý cả IPv6 và IPv4. Mỗi tài nguyên sẽ có nhiều thông số thể hiện như Hệ điều hành, tên, phiên bản để người quản trị dễ dàng xem thông tin. ✓ Lỗ hổng bảo mật: cho phép tính toán và đưa ra điểm theo chuẩn CVSS về mức độ nguy hiểm dựa trên việc dễ dàng

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn(*)
		tấn công, dễ dàng đăng nhập hay các thông tin khác. Điểm cho mỗi lỗ hổng bảo mật được tính từ 1-10 và được dùng cho PCI (Payment Card Industry) ✓ Báo cáo: - Cho phép báo cáo theo từng nhóm tài nguyên. - Cho phép tạo báo cáo cơ bản: lựa chọn kiểu báo cáo, lựa chọn báo cáo ra tài liệu (Text, PDF, RTF, HTML). - Lựa chọn Export báo cáo được thiết kế phù hợp với các hệ thống khác, dạng báo cáo có thể bao gồm theo XML, Database Export và CSV. ✓ Hỗ trợ khai thác lỗ hổng bảo mật để đánh giá lại ảnh hưởng khi lỗ hổng bảo mật bị tấn công: - Chương trình hỗ trợ cho phép khai thác lỗ hổng bảo mật qua giao diện: Command-line, Web Interface. - Hỗ trợ khai thác thông minh (Smart Exploition). - Kiểm tra việc đặt mật khẩu (Password Auditing). - Đưa ra báo cáo. - Quản lý dữ liệu (Data Management). - Chương trình khai thác cho phép kết hợp với các chương trình phát hiện mạng và cho phép nhập kết quả từ hãng thứ 3 (Network Discovery and third-party import). ▪ Tương thích: ✓ Phần mềm dò quét có khả năng triển khai trên các hệ điều hành: Microsoft Windows Server 2008 R2, Windows Server 2012 (64-bit), Windows 7 and Windows 8 (64-bit), VMware ESX 3.5 and 4.0, ESXi 3.5, 4.0 and 5.0, Red Hat Enterprise Linux 5.x, 6.x, Ubuntu Linux 10.04 LTS (64 bit only), Ubuntu 12.04 LTS (64 bit only).
6.	Gia hạn bản quyền phần mềm diệt virus (12 tháng)	- Chủng loại: Bản quyền phần mềm diệt virus phiên bản dành cho doanh nghiệp Kaspersky Endpoint Security *hoặc tương đương*. - Thời hạn sử dụng: 12 tháng kể từ ngày kích hoạt. *Chất lượng sản phẩm:* ▪ Là sản phẩm có uy tín, được kiểm định, chứng nhận của các tổ chức đánh giá độc lập về phần mềm diệt virus như Virus Bulettin, AV-Test, AV Comparatives hoặc đánh giá trong nhóm dẫn đầu về sản phẩm phòng chống virus của Gartner. *Chủng loại sản phẩm:* ▪ Sản phẩm phòng chống virus phiên bản dành cho doanh nghiệp, thực hiện bảo vệ các máy tính chủ, máy tính trạm của Tòa soạn

TT	Danh mục dịch vụ	Thông số kỹ thuật và các tiêu chuẩn(*)
		trước các nguy hại do virus gây ra. *Tính năng cơ bản của sản phẩm:* ▪ Khả năng quản lý tập trung: ✓ Khả năng cài đặt phần mềm diệt virus lên máy tính từ xa thông qua các máy chủ cài đặt phần mềm quản trị tập trung của sản phẩm. ✓ Khả năng quản lý, điều khiển phần mềm diệt virus trên máy tính từ xa qua phần mềm quản trị tập trung. ✓ Khả năng thiết lập mô hình quản lý phân cấp, qua đó phân quyền quản trị cho các đơn vị cấp dưới theo phạm vi đơn vị phụ trách. ▪ Tích hợp với hệ thống quản lý người dùng (AD/LDAP), bảo vệ máy tính: ✓ Phòng chống và tiêu diệt các loại virus, spyware, malware, macro... ✓ Chức năng tường lửa bảo vệ cho máy tính trước các hành vi xâm nhập, tấn công, truy nhập bất hợp pháp. ▪ Thiết lập các chính sách sử dụng internet cho các máy tính sử dụng phần mềm diệt virus. ▪ Thiết lập chính sách diệt virus theo nhóm máy tính. ▪ Quản lý ứng dụng: khả năng chặn các ứng dụng mà nhân viên không được phép sử dụng theo chính sách đặt ra. ▪ Quản lý hoạt động của các phần mềm chạy trên máy tính. ▪ Quản lý thiết bị ngoại vi: thực hiện khóa các thiết bị ngoại vi như USB, ổ cứng di động... kết nối đến máy tính theo chính sách đặt ra. ▪ Hỗ trợ nhiều hệ điều hành khác nhau dành cho máy chủ, máy trạm: windows, linux, mac,... ▪ Hỗ trợ phòng chống virus trên môi trường ảo hóa.

(*)*Ghi chú:* Trường hợp nhà thầu đề xuất giải pháp công nghệ, kỹ thuật khác so với yêu cầu thì nhà thầu cần chứng minh kèm theo tài liệu:

- Tính tương đương và vượt trội về công nghệ của giải pháp kỹ thuật khác đó trong việc đảm bảo khai thác sử dụng hiệu quả theo các yêu cầu của gói thầu (có kèm theo tài liệu để chứng minh).

- Tính tương thích của giải pháp kỹ thuật khác đó ứng dụng trên hạ tầng phần cứng và phần mềm của Báo Quân đội nhân dân hiện có là hoàn toàn tương thích, phù hợp, không gây xung đột mà vẫn đảm bảo an toàn, hiệu quả, hiệu năng khai thác sử dụng hệ thống.

4. Quy định về kiểm tra, nghiệm thu sản phẩm:

Các kiểm tra cần tiến hành gồm có:

- Kiểm tra chung về dịch vụ (hãng cung cấp, chủng loại, nguồn gốc...).

- Kiểm tra thông số kỹ thuật (tính năng, chức năng) của dịch vụ, phần mềm.

Vận hành thử nghiệm các tính năng đảm bảo chất lượng và đặc tính kỹ thuật đáp ứng yêu cầu của hợp đồng.

- Phối hợp kiểm tra và nghiệm thu theo quy định của Bộ Quốc phòng.

5. Các yêu cầu khác:

- Nhà thầu phải là đơn vị có kinh nghiệm, đã từng triển khai, cung cấp các dịch vụ trên nền tảng công nghệ của Imperva, Citrix và Sophos từ năm 2023 trở lại đây.

- Nhà thầu phải chịu hoàn toàn trách nhiệm về việc cung cấp dịch vụ của gói thầu khi triển khai trên hạ tầng của Báo Quân đội nhân dân nếu xảy ra sự cố hệ thống dẫn đến ảnh hưởng, gián đoạn quy trình sản xuất, xuất bản của Tòa soạn.

- Nhà thầu phải chịu hoàn toàn trách nhiệm nếu có bất kỳ khiếu kiện của bên thứ ba về vấn đề bản quyền của các dịch vụ cung cấp cho gói thầu này.

- Trong suốt thời gian thực hiện hợp đồng 12 tháng, nhà thầu cần:

+ Bố trí nhân sự hỗ trợ kỹ thuật 24giờ/ngày+7ngày/tuần trong suốt thời gian thực hiện hợp đồng 12 tháng.

+ Cam kết xử lý sự cố trong vòng 01 giờ kể từ khi nhận được yêu cầu của đơn vị sử dụng vào bất kỳ thời điểm nào.

+ Tiến hành kiểm tra, bảo trì, và tối ưu hóa hệ thống vào ngày đầu tiên hàng tháng.