BỘ Y TẾ **BỆNH VIỆN HỮU NGHỊ VIỆT ĐỨC**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 2976/VĐ-CNTT V/v Mua sắm thiết bị tường lửa bảo vệ kết nối an toàn dữ liệu giữa cơ sở Tràng Thi và cơ sở Ngọc Hồi	*Hà Nội, ngày 12 tháng 05 năm 2026*

Kính gửi: Các công ty/ đơn vị /nhà cung cấp

Hiện nay, Bệnh viện Hữu nghị Việt Đức có nhu cầu tiếp nhận báo giá để tham khảo, xây dựng giá gói thầu, làm cơ sở tổ chức lựa chọn nhà thầu cung cấp hàng hóa với nội dung cụ thể như sau:

I. Thông tin của đơn vị yêu cầu báo giá

1. Đơn vị yêu cầu báo giá: Bệnh viện Hữu nghị Việt Đức
2. Thông tin liên hệ của người chịu trách nhiệm tiếp nhận báo giá: Phòng Công nghệ thông tin – Bệnh viện Hữu nghị Việt Đức; Số 40 – Tràng Thi – Hoàn Kiếm – Hà Nội. Thông tin cần giải đáp xin liên hệ:
   - Người nhận báo giá: Trần Tuấn Anh (Nhân viên phòng Công nghệ thông tin)
   - Điện thoại: 0243.8253531-5469 – Email: cntt@vduh.org
   - Di động: 0364.169.099
3. Bệnh viện tiếp nhận báo giá **đồng thời theo 2 hình thức**
   - Nhận trực tiếp tại địa chỉ: Phòng Công nghệ thông tin – Tầng 7 nhà H –Trung tâm Khám bệnh – Cấp cứu và Điều trị trong ngày, Số 40 – Tràng Thi – Hoàn Kiếm – Hà Nội.
   - Nhận qua email: Email: vietduchospitalmuasam@gmail.com và cntt@vduh.org (Ghi rõ số hiệu văn bản Bệnh viện ban hành, đính kèm bản mềm chào giá của công ty/đơn vị/nhà cung cấp)
4. Thời hạn tiếp nhận báo giá: từ 08h ngày 14 tháng 05 năm 2026 đến trước 08h ngày 24 tháng 05 năm 2026.

   Các báo giá nhận được sau thời điểm nêu trên sẽ không được xem xét.
5. Thời hạn có hiệu lực của báo giá: Tối thiểu 90 ngày

II. Nội dung yêu cầu báo giá:

1. Danh mục hàng hóa.
2. Địa điểm cung cấp, lắp đặt các yêu cầu về vận chuyển, cung cấp, lắp đặt, bảo quản hàng hóa tại phòng Công nghệ thông tin – Bệnh viện Hữu nghị Việt Đức.
3. Thời gian giao hàng dự kiến: Trong vòng 07 ngày kể từ khi có yêu cầu.
4. Thời gian thanh toán tối đa 90 ngày kể từ khi bên bán cung cấp đầy đủ chứng từ hợp lệ theo quy định cho bên mua hàng.
5. Các thông tin khác
   - Đăng ký kinh doanh;
   - Số điện thoại/Email của đại diện đơn vị báo giá trong trường hợp Bệnh viện cần liên lạc;
   - Bảng chào giá *(theo mẫu đính kèm tại phụ lục công văn này);*
   - Niêm yết giá *(nếu có);*
   - Catalog, hợp đồng tương tự (nếu có), cấu hình và tính năng kỹ thuật của vật tư và các tài liệu khác liên quan;
   - Báo giá phải bao gồm thuế VAT;
   - Hàng hóa cung cấp phải cam kết có nguồn gốc xuất xứ rõ ràng;
   - Báo giá có chữ ký và đóng dấu đầy đủ;

Rất mong nhận được sự tham gia của các đơn vị

Trân trọng!

Nơi nhận:
- Như trên;
- Lưu: VT; CNTT.

TL.GIÁM ĐỐC
KT.TRƯỞNG PHÒNG CÔNG NGHỆ THÔNG TIN
PHÓ TRƯỞNG PHÒNG

BỆNH VIỆN HỮU NGHỊ VIỆT ĐỨC

Nguyễn Ngọc Toàn

PHỤ LỤC

DANH MỤC HÀNG HÓA

(Đính kèm công văn 2976 /VĐ- CNTT ngày 14/05/2026)

STT	Danh mục	Mô tả	Đơn vị tính	Số lượng	Nhãn hiệu/ Hãng sản xuất/ Xuất xứ	Đơn Giá	Thành tiền
1	**Thiế bị tường lửa đặt tại cơ sở Tràng Thi**	Cổng mạng: ≥ 12 x 1G/2.5G/5G/10G RJ45; ≥ 10 x 1G/10G SFP/SFP+ ; ≥ 4 x 25G SFP28 Cổng HA: ≥ 3 cổng chuyên dụng cho đồng bộ HA Cổng quản trị: ≥ 01 cổng management RJ45; ≥ 01 MicroUSB Console Hỗ trợ High Availability (HA) Active/Passive hoặc Active/Active: Có Thông lượng appmix: ≥ 13 Gbps Thông lượng Threat prevention: ≥ 7 Gbps Phiên (Sessions) đồng thời: ≥ 1.4 triệu Số phiên mới trên mỗi giây: ≥ 140.000 Bộ định tuyến ảo (Virtual Router) ≥ 10; Hệ thống ảo (Virtual systems) ≥ 10; Vùng bảo mật (Security Zone) ≥ 1.000; Đường dây ảo (Virtual Wire) ≥ 1.000 Có khả năng tích hợp với các hệ thống cung cấp danh sách IP/URL độc hại bên ngoài với số lương tối thiểu ≥ 30 Dịch vụ bảo vệ: IPS, Malware protection, URL filtering Có khả năng giải mã SSL/TLS Có tính năng chia sẻ luồng dữ liệu đã giải mã ra ngoài qua port mirror Có tính năng Network Packet Broker để giải mã và chia sẻ dữ liệu một chuỗi các thiết bị bảo mật khác theo mô hình Layer 3 hoặc Transparent. Hỗ trợ mã hoá IPSE, SSL VPN	Cái	1			

		Hỗ trợ mã hoá lượng tử (Post-Quantum Cryptography) với các thuật toán như ML-KEM, ML-DSA, and SLH-DSA, Có Cloud sandbox hoặc tương đương Hỗ trợ SD-WAN Hỗ trợ syslog, API, SIEM Nguồn: ≥ 02 nguồn AC dự phòng Kiểm soát ứng dụng và người dùng: Có khả năng nhận dạng và kiểm soát ứng dụng, người dùng. Có tính năng giúp tối ưu các chính sách an ninh, chuyển đổi từ sử dụng port base sang ứng dụng (Application) ngay trên thiết bị Có nhiều cơ chế định danh người dùng như Server monitoring, Port mapping, syslog, XFF Header, Username Header Insertion, Authentication policy, XML API, Client probing Hỗ trợ nhận thông tin về người dùng qua Syslog trực tiếp trên thiết bị Tính năng ngăn chặn tấn công: Có tính năng vulnerability protection/IPS trên thiết bị đề xuất, đồng thời với antivirus và anti-spyware Sử dụng các mô hình học sâu nội tuyến (inline deep learning) để ngăn chặn các lưu lượng C2 lẩn tránh và chưa được biết đến từ các công cụ Red Team phổ biến như Cobalt Strike và Empire. Có khả năng phát hiện và ngăn chặn các tấn công Command Injection và SQL Injection chưa biết (unknown) Phát hiện và ngăn chặn các kết nối C2C, sử dụng DNS sinkholing để xác định các máy bị lây nhiễm Có khả năng lọc file và dữ liệu Tính năng phân tích động các file nghi ngờ:					

		Có tính năng tính năng phân tích động và tạo threat signature cho các loại file: apk, pe , pdf, office, elf, rar, 7z, JS, VBS, eml và Shell script Có mô hình học máy nội tuyến (inline) gọn nhẹ trên NGFW cung cấp khả năng ngăn chặn theo thời gian thực đối với các mã độc (malware) đã biết và các biến thể chưa biết. Có khả năng giám sát tàng hình (stealthy observation) để tránh bị phát hiện phân tích các loại malware có khả năng phát hiện môi trường sandbox Có khả năng đánh giá toàn bộ hành vi mạng (network activity) phát sinh từ một tập tin khả nghi, như hành vi khởi tạo backdoor, tải xuống các next-stage malware Phát hiện tấn công Fileless/Script Có tính năng cập nhật signature mới real time ngay sau khi Threat cloud phân tích và xác định xong mẫu Tính năng kiểm soát truy cập web: Cung cấp sẵn hơn 70 danh mục web và cho phép tự bổ sung thêm các danh mục theo nhu cầu thực tế Phân tích và ngăn chặn URL độc hại theo thời gian thực (Real-time Web/URL Filtering), Ứng dụng công nghệ học máy để phân tích web traffic, nhằm phát hiện và ngăn chặn tức thời các tấn công chưa biết (bao gồm phishing, exploits, fraud và C2). Phát hiện giả mạo thương hiệu bằng hình ảnh (Image-based Brand Impersonation Detection), ứng dụng các mô hình học máy (ML) để phân tích hình ảnh trên webpage nhằm nhận diện các dấu hiệu giả mạo thương hiệu trong các cuộc tấn công phishing.					

		Có tính năng kiểm soát việc gửi thông tin đăng nhập nội bộ (corporate credentials) dựa trên URL category. Phải có khả năng chặn hành vi nhập thông tin xác thực trên các trang không tin tưởng theo thời gian thực (real-time) Có khả năng p hân loại URL theo nhiều danh mục (Multicategory Support) lên đến 04 categories đồng thời, cho phép cấu hình policy linh hoạt. License bảo mật: Bao gồm bản quyền cập nhật các tính năng bảo mật tối thiểu 3 năm Bảo trì: Hỗ trợ chính hãng tối thiểu 3 năm					
2	**Thiết bị tường lửa đặt tại cơ sở Ngọc Hồi**	Cổng mạng: ≥ 8 x GE copper; ≥ 2 x SFP fiber; ≥ 2 x SFP+ 10 GE fiber; Số lượng module mở rộng ≥ 1 Cổng quản trị: ≥ 1 x RJ45 MGMT; ≥ 1 x COM RJ45 hoặc 1 x Micro-USB; ≥ 2 x USB 3.0 Thông lượng IMIX ≥ 27 Gbps Độ trễ firewall: ≤ 4 microsecond Thông lượng IPS ≥ 14 Gbps Thông lượng bảo vệ khỏi các mối nguy hại: ≥ 10 Gbps Thông số NGFW ≥ 12,5 Gbps Kết nối đồng thời tối đa ≥ 13.700.000 Số kết nối mới mỗi giây ≥ 257.800 Số tunnel đồng thời cho IPsec VPN ≥ 6.500 Thông lượng kiểm tra SSL/TLS ≥ 3,13 Gbps Kết nối đồng thời SSL/TLS ≥ 102.400 Vi xử lý: x86 AMD CPU và Marvell NPU hoặc tương đương Màn hình hiển thị: Multi-function LCD module Kiểu dáng: Rackmount Hỗ trợ quản trị thông qua giao diện web GUI, CLI và Cloud Central Hỗ trợ xác thực 2 nhân tố cho truy cập quản trị, kết nối IPSec và SSL VPN.	Cái	1			

		Có hỗ trợ trang quản trị cho người dùng cuối User Portal Hỗ trợ sao lưu và Phục hồi cấu hình Hỗ trợ tích hợp API của bên thứ 3 Hỗ trợ High Avaibility theo chế độ active/passive, active/active, chuyển đổi trạng tháiHA cho kết nối IPsec đối với RBVPN, PBVPN và VPN truy cập từ xa mà không mất phiên sự kiện Hỗ trợ Zero-Touch deployment Kiến trúc xử lý: Sử dụng kiến trúc xử lý gói tin thông minh để phát hiện mã độc và bảo vệ hệ thống; Hỗ trợ giải mã lưu lượng TLS 1.3 mà không hạ bậc giao thức; Hỗ trợ DPI Engine; Hỗ trợ tự động tăng tốc thông minh các lưu lượng đáng tin cậy Tính năng mạng: Ngăn chặn các tấn công DoS và portscan; Chặn lưu lượng theo vùng địa lý; Chính sách theo mạng/người dùng/thời gian/vùng mạng; Cân bằng tải nhiều đường Internet; Hỗ trợ giao thức định tuyến tĩnh, multicast và động (RIP, BGP, OSPF);Hỗ trợ giao thức 802.3ad (LAG) Tính năng xác thực: Hỗ trợ xác thực thông qua Active Directory hoặc RADIUS hoặc TACACS; Hỗ trợ Single Sign-On: Active directory, hoặc RADIUS Accounting Tính năng VPN: Hỗ trợ giao thức VPN site-to-site; Truy cập từ xa bằng giao thức VPN; Hỗ trợ Route-based VPN; Hỗ trợ đồng bộ bảo mật và khả năng phối hợp thông tin giữa người dùng và tường lửa cho kết nối từ xa; Hỗ trợ khả năng chia tách đường hầm thông minh để định tuyến lưu lượng tối ưu Tính năng SD-WAN: Hỗ trợ nhiều kết nối WAN, các tùy chọn bao gồm VDSL, DSL, cáp ,					

		LTE/Cellular, và MPLS; Hỗ trợ chọn đường và định tuyến theo ứng dụng Tính năng bảo vệ mạng và phòng chống xâm nhập: Hỗ trợ tích hợp hệ thống chống xâm nhập IPS với hàng nghìn mẫu dấu hiệu có sẵn Hỗ trợ tùy chỉnh mẫu dấu hiệu IPS Công nghệ kết hợp giữa Firewall và endpoint cùng hãng để phòng chống lại mối đe doạ nâng cao Hỗ trợ tự động ngăn chặn mọi traffic từ các máy đầu cuối bị nhiễm mã độc khi cài endpoint của hãng Tự động giám sát và chặn các mối đe dọa APT và các mối đe dọa khác được xác định thông qua các nguồn cấp dữ liệu Threat Feeds, cung cấp bảo vệ nâng cao khỏi các bot và đối thủ chủ động cố gắng liên hệ đến các điểm đến độc hại bằng cách sử dụng phát hiện đa lớp Hỗ trợ VPN không cần cài Agent Tính năng bảo vệ người dùng truy cập web: Hỗ trợ quét mã độc trên giao thức HTTP/S, FTP và webmail Hỗ trợ cơ sở dữ liệu bộ lọc URL với hơn 90 loại danh mục web Hỗ trợ chính sách định mức truy cập web theo người dùng/nhóm người dùng Hỗ trợ phát hiện mã độc sử dụng nhiều AV engine Hỗ trợ đánh giá mức độ nguy hại của người dùng Hỗ trợ giới hạn băng thông theo ứng dụng, theo danh mục Web Hỗ trợ ngăn chặn các ứng dụng không mong muốn					

		Bảo vệ nâng cao trước phần mềm độc hại trên web với trình mô phỏng JavaScript. Hỗ trợ quản lý chính sách ứng dụng theo User và Network License bảo mật: Bao gồm bản quyền cập nhật các tính năng bảo mật tối thiểu 3 năm Bảo trì: Hỗ trợ chính hãng tối thiểu 3 năm					

Yêu cầu khác:

Hàng hóa phải có nguồn gốc, xuất xứ rõ ràng; được sản xuất năm 2025 trở về sau.

Hàng hóa bao gồm đầy đủ linh phụ kiện đảm bảo cho triển khai;

Nhân sự triển khai có trình độ về bảo mật tối thiểu:

- Có tối thiểu một nhân sự tổng phụ trách kỹ thuật, tốt nghiệp đại học chuyên ngành Công nghệ thông tin hoặc Điện tử viễn thông sở hữu các chứng chỉ sau: CISSP, CCIE Enterprise Infrastructure, CCDE (Còn hiệu lực)
- Có tối thiểu một nhân sự phụ trách triển khai, tốt nghiệp đại học chuyên ngành Công nghệ thông tin hoặc Điện tử viễn thông sở hữu các chứng chỉ sau: CCIE Security (Còn hiệu lực)