Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

1.1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu

- Tên gói thầu: Gói thầu số 02 - Mua sắm trang thiết bị.
- Tên Dự toán: Mua sắm trang thiết bị của Cổng thông tin điện tử năm 2026.
- Chủ đầu tư: Cổng thông tin điện tử thành phố huế.
- Địa điểm thực hiện: Số 16 Lê Lợi, phường Thuận Hoá, thành phố Huế.
- Hình thức LCNT: Chào hàng cạnh tranh thông thường, trong nước qua mạng.
- Phương thức LCNT: Một giai đoạn, một túi hồ sơ.
- Loại hợp đồng: Trọn gói.
- Nguồn vốn: Ngân sách nhà nước.
- Thời gian thực hiện: 30 ngày.

1.2. Yêu cầu về kỹ thuật

STT	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn
1	Thiết bị tên lửa	Thiết bị tường lửa: Firewall throughput: 79.5 Gbps; Maximum Sessions: 7.800.000; New Session per Second: 500.000; IPsec VPN throughput: 55 Gbps; Dung lượng lưu trữ: 2*480 GB SSD; Số cổng RJ45 built-in: 16 GE RJ45 Ports + 2 x GE RJ45 MGMT/HA Ports; Số slot giao tiếp SFP: 8; Số slot giao tiếp SFP+: 8; Số cổng Console: 01; Số cổng USB: 01; Hỗ trợ 2 nguồn (có khả năng dự phòng nguồn); Tính năng: Cung cấp hiệu suất lọc bảo mật và kiểm tra dữ liệu mã hóa SSL; Tích hợp phần mềm và phần cứng vượt trội đảm bảo sử dụng tối ưu các thành phần phần cứng; Web & Video Filtering: 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: Hơn 250 triệu URLs được đánh giá vào 78 thể loại web với 70 ngôn ngữ, 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 and DoS: IPS Engine: hơn 11,000 signatures và cập nhật với nhà sản xuất, phát hiện giao thức bất thường, ngưỡng bất thường, signature tự định nghĩa; Anti-Malware: 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; FortiOS Datasheet: AI-based malware detection: module is trained by FortiGuard AV against many malware samples to identify file features that make up the malware FortiOS 7.2 Admin Guide: The AV Engine AI malware detection model integrates into regular AV scanning to help detect potentially malicious Windows Portable Executables (PEs) in order to mitigate zero-day attacks; Automation: Hỗ trợ chức năng tự động hoá: quản trị viên lập trình sẵn hành vi phản ứng khi có các sự cố (incident/ event), ví dụ cách ly host khi phát hiện lây nhiễm; Gởi email, cảnh báo đến quản trị viên hoặc tự động thực hiện CLI Script khi CPU sắp quá tải/ có thay đổi trên cấu hình thiết bị… để đơn giản công tác quản trị, các khai báo tự động hoá này phải được thiết lập trên cùng một trang giao diện quản lý (GUI); 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; VPN: Auto Discovery VPN (ADVPN): Tự động thiết lập Tunnel kết nối (gọi là 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; The transparent conditional DNS forwarder allows the FortiGate to intercept and reroute DNS queries for specific domains to a specific DNS server; This provides greater control over DNS requests, especially when the administrator is not managing the DNS server configuration of the client

		devices; VPN: Hỗ trợ triển khai theo các chế độ: Gateway-to-Gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN terminate in transparent mode; SD WAN: 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: 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; Hỗ trợ tính năng cân bằng tải server thông với nhiều phương thức: Tĩnh (Failover), Round Robin, Weighted Round Trip Time, số lượng Connections; Hỗ trợ tính năng cân bằng tải server thông với nhiều giao thức: HTTP, HTTPS, IMAPS, POP3S, SMTPS, SSL hoặc các giao thức được định nghĩa dựa trên TCP/UDP; SD WAN: Hỗ trợ đo lường hiệu suất đường truyền theo hình thức bị động: đo lường hiệu suất đường truyền dựa theo thông tin session được ghi nhận bởi các chính sách tường lửa; Application Control: Phát hiện hàng ngàn ứng dụng trong nhiều categories: 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; IPS and DoS: 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); Hỗ trợ cơ chế HA: Active-passive, active-active, virtual clusters, VRRP; + Thiết bị có đầy đủ bản quyền sử dụng các tính năng Unified Threat Protection (IPS, Anti-Malware Protection, Application Control, URL DNS và Video

		Filtering, Antispam) thời hạn 1 năm; + Thiết bị có đầy đủ bản quyền sử dụng các tính năng Advanced Malware Protection - Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection và Sandbox Cloud Service thời hạn 1 năm; + Dịch vụ bảo hành phần cứng và hỗ trợ kỹ thuật của hãng sản xuất, thời hạn 1 năm. Bao gồm: Chuyển đổi cấu hình một lần cho model FortiGate 401F (Đảm bảo chuyển đổi đủ tất cả tài khoản/mật khẩu đã tạo từ trước trên SSL-VPN model FortiGate 300C): FortiConverter Service offers an intuitive cloud portal for third-party firewall migration. Simply upload the source configuration files and let FortiConverter does the rest. You also have visibility of service entitlement and status across all FortiGate devices. Ghi chú: Sản phẩm có giấy chứng nhận chất lượng CQ trực tiếp của nhà sản xuất cấp cho EU.

1.3. Các yêu cầu khác

- Tiến độ cung cấp hàng hóa: 30 ngày;

- Địa điểm cung cấp: Số 16 Lê Lợi, phường Thuận Hoá, thành phố Huế

Mục 2. Bản vẽ: Không có bản vẻ kèm theo.

Mục 3. Kiểm tra và thử nghiệm

Các kiểm tra và thử nghiệm cần tiến hành gồm có:

Kiểm tra hàng hóa khi giao hàng:

- Kiểm tra tại chỗ hàng hóa được bàn giao về số lượng, chủng loại, xuất xứ, nhãn hàng hóa.

- Kiểm tra sơ bộ đóng gói bên ngoài

- Nếu kết quả kiểm tra về số lượng, chủng loại, xuất xứ, quy cách hàng hóa chứng tỏ rằng hàng hóa phù hợp với Hợp đồng thì hai bên sẽ tiến hành ký Biên bản kiểm tra hàng hóa

- Các quy định khác theo quy định.