Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. Yêu cầu về kỹ thuật

Mục 1. Yêu cầu về kỹ thuật

1. Giới thiệu chung về dự án, gói thầu

- Tên dự toán: "Mua sắm thay thế thiết bị firewall của Học viện Công nghệ Bưu chính Viễn thông".
- Tên gói thầu: Mua sắm thay thế thiết bị firewall của Học viện Công nghệ Bưu chính Viễn thông
- Gói thầu được tổ chức để mua sắm: Thiết bị firewall của Học viện Công nghệ Bưu chính Viễn thông
- Địa điểm thực hiện: Gói thầu được thực hiện tại Thành phố Hà Nội.
- Thời gian thực hiện gói thầu: Thời gian thực hiện là 40 ngày, trong đó dự kiến như sau:

STT	Nội dung công việc	Thời gian thực hiện (ngày)
1	Thời gian giao hàng	40
2	Thời gian triển khai và nghiệm thu	
	Tổng thời gian	**40**

2. Yêu cầu chung:

2.1. Yêu cầu về tuyên bố đáp ứng

Yêu cầu về kỹ thuật cho hàng hóa mời thầu gồm các thông tin nội dung và yêu cầu kỹ thuật chi tiết cho từng nội dung, chi tiết theo bảng trong mục 3.1. Mỗi yêu cầu kỹ thuật được mô tả mức độ yêu cầu đáp ứng rõ ràng.

Để chứng minh tính đáp ứng yêu cầu kỹ thuật, nhà thầu được yêu cầu tuyên bố hàng hóa mình chào thầu "Đáp ứng" hay "Không đáp ứng" các yêu cầu kỹ thuật trong "Bảng tuyên bố đáp ứng các yêu cầu kỹ thuật".

Bảng tuyên bố đáp ứng các yêu cầu kỹ thuật được lập dạng bảng gồm tối thiểu các thông tin với cấu trúc sau:

TT	Nội dung	Yêu cầu kỹ thuật	Tuyên bố đáp ứng	Thông tin chứng minh
(1)	(2)	(3)	(4)	(5)

Trong đó:

- Cột (1), (2), (3) lấy theo yêu cầu kỹ thuật trong E-HSMT
- Cột (4) ghi tuyên bố: "Đáp ứng" hoặc "Không đáp ứng". Trường hợp nhà thầu tuyên bố là "Không đáp ứng" thì yêu cầu kỹ thuật đó sẽ bị đánh giá là "Không đạt".
- Cột (5) giải thích lý do tuyên bố đáp ứng hoặc không đáp ứng và cung cấp tài liệu chứng minh. Nhà thầu phải chỉ rõ tên tài liệu, mục, trang, dòng của tài liệu chứng minh. Nhà thầu phải chịu trách nhiệm về tính chính xác của các tài liệu mình cung cấp, trường hợp Bên mời thầu phát hiện các tài liệu cung cấp không đúng sự thật, thì Nhà thầu sẽ được đánh giá là gian lận và bị loại.

2.2. Yêu cầu về cung cấp tài liệu kỹ thuật

- Nhà thầu liệt kê chi tiết và giải thích bằng tiếng Việt toàn bộ các thành phần:
  + Các phần mềm, tính năng, dịch vụ hỗ trợ kỹ thuật, license có sẵn hoặc đã được nhà thầu cung cấp theo gói thầu.
  + Các phần mềm, tính năng, dịch vụ hỗ trợ kỹ thuật, license có hỗ trợ nhưng không cung cấp theo gói thầu và cần phải mua bổ sung nếu muốn sử dụng.
- Nhà thầu phải cung cấp giải pháp kỹ thuật mô tả chi tiết các thành phần như sau:
  + Triển khai lắp đặt hạ tầng thiết bị.
  + Thiết kế LLD và cấu hình thiết bị Firewall

3. Yêu cầu kỹ thuật chi tiết hàng hóa:

3.1. Yêu cầu kỹ thuật chi tiết của hàng hóa, dịch vụ:

(Chi tiết như Phụ lục 1 kèm theo)

3.2. Yêu cầu về tiến độ thực hiện gói thầu

- Thời gian giao hàng và triển khai thi công lắp đặt, cấu hình hệ thống: Tối đa 40 ngày.
- Địa điểm giao hàng và triển khai lắp đặt hàng hóa: Tầng 1 nhà A3, cơ sở đào tạo Hà Đông, 96A Trần Phú, Hà Đông, Hà Nội.

3.3. Yêu cầu về hàng hóa, dịch vụ:

a. Thời gian, địa điểm bảo hành

Nhà thầu phải cam kết đáp ứng các yêu cầu tối thiểu như sau:

- Thời gian bảo hành: 1 năm theo tiêu chuẩn của nhà sản xuất.
- Địa điểm bảo hành: Toàn bộ hàng hóa được bảo hành tại địa điểm lắp đặt của Chủ đầu tư.
- Chính sách bảo hành: Bảo hành chính hãng

b. Cam kết hỗ trợ từ hãng

Nhà thầu phải cung cấp hỗ trợ từ hãng sản xuất.

c. Tài liệu chứng minh tính hợp lệ của hàng hóa:

+ Giấy chứng nhận xuất xứ hàng hóa (CO), Giấy chứng nhận chất lượng hàng hóa (CQ) hoặc các giấy tờ khác tương đương chứng minh tính hợp lệ về nguồn gốc, xuất xứ, chất lượng của hàng hóa.

+ Phiếu bảo hành, Biên bản kiểm tra xuất xưởng của nhà sản xuất (nếu có)

d. Quy trình thực hiện

- Có quy trình các bước thực hiện lắp đặt, chuyển đổi cấu hình từ thiết bị firewall Fortinet 600D đang sử dụng lên thiết bị firewall mới.

e. Các cam kết khác

- Cam kết tiến độ triển khai dịch vụ đúng yêu cầu của E-HSMT.
- Cam kết thời gian giãn đoạn dịch vụ (downtime) <= 2h (2 tiếng)
- Cam kết thiết bị firewall mới tương thích và chuyển đổi toàn bộ cấu hình, dịch vụ trên thiết bị cũ (Firewall fortinet 600D) lên thiết bị firewall mới hoạt động bình thường.

Mục 2. Bản vẽ: Không có.

Mục 3. Kiểm tra và thử nghiệm: Không có.

PHỤ LỤC 1 - YÊU CẦU KỸ THUẬT CHI TIẾT CỦA HÀNG HÓA VÀ DỊCH VỤ

STT	NỘI DUNG	YÊU CẦU
A	**THIẾT BỊ FIREWALL, LICENSE, MODULE, DÂY QUANG**	
I	**THIẾT BỊ FIREWALL**	
1	Thông tin hãng sản xuất	Nhà sản xuất thiết bị phải thuộc nhóm Leader trong đánh giá: Gartner Magic Quadrant Network Firewall 3 năm gần nhất
		Giải pháp nằm trong nhóm leader theo đánh giá mới nhất: Gartner® Magic Quadrant™ for Hybrid Mesh Firewall
2	**Thông tin về phần cứng**	
2.1	Hiệu suất và năng lực	Thông lượng Firewall ≥ 164 Gbps
2.2		Firewall Latency ≤ 3.87 µs
2.3		Firewall Throughput (Packet Per Second) ≥ 217.5 Mpps
2.4		Maximum Sessions ≥ 16000000
2.5		New Sessions(Connections)/Sec ≥ 140000
2.6		Firewall Policies ≥ 10 000
2.7		Thông lượng IPSec VPN ≥ 55 Gbps
2.8		SSL VPN Throughput ≥ 8 Gbps
2.9		SSL/TLS Inspection Throughput ≥ 14 Gbps
2.10		IPS Throughput ≥ 38 Gbps
2.11		NGFW Throughput ≥ 29 Gbps
2.12		Thông lượng Threat Prevention ≥ 26 Gbps
2.13		Application Control Throughput ≥ 50 Gbps
2.14	Giao diện hỗ trợ	Số cổng RJ45 built-in ≥ 8
2.15		Số slot giao tiếp SFP ≥ 16
2.16		Số slot giao tiếp SFP+ ≥ 8
2.17		Số cổng USB ≥ 2
2.18		Số cổng Console ≥ 1
2.19	Nguồn điện	Hỗ trợ 2 nguồn
2.20	Tích hợp SSD storage	Tối thiểu 960Gb
3	**Tính năng**	
3.1	Kiến trúc phần cứng	Tích hợp với kiến trúc phần cứng độc quyền bao gồm các thành phần tăng tốc (SPU) và bộ xử lý đa lõi. Tích hợp phần mềm và phần cứng vượt trội đảm bảo sử dụng tối ưu các thành phần phần

		cứng, mang lại chi phí / hiệu suất cao nhất cho khách hàng.
3.2	Tính năng IPS	Hộ trợ tính năng IPS để ngăn chặn các dạng tấn công mạng dựa theo thông tin nhận diện được cập nhật từ hãng sản xuất và cho phép quản trị viên tự định nghĩa thông tin nhận diện
3.3	Tính năng Antivirus	Hỗ trợ tính năng Antivirus để lọc virus/malware qua các kênh truyền mạng như HTTP, FTP, SMTP, IMAP, POP3
3.4	Application Control	Tính năng Application Control: Hỗ trợ phát hiện hàng ngàn ứng dụng, có khả năng tùy chỉnh thông tin nhận diện ứng dụng.
3.5	Tính năng VPN	Hỗ trợ tính năng 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.
		Hỗ trợ tính năng IPSec Aggregate tunnels: Hỗ trợ cân bằng tải trên từng gói tin (Per-packet) theo các thuật toán: IP Addresses, L4 information và (weighted) round-robin.
3.6	Tự động hóa	Automation: Hỗ trợ tự động hoá cho phép quản trị viên định nghĩa phản ứng khi có sự cố, ví dụ: cách ly host, gửi cảnh báo, thực hiện CLI Script… Tất cả được cấu hình và quản lý tập trung trên cùng một giao diện GUI.
3.7	Cơ chế HA	Hỗ trợ cơ chế HA: Active-passive, active-active, virtual clusters, VRRP
3.8	Bản quyền sử dụng	Thiết bị có đầy đủ bản quyền sử dụng các tính năng IPS, Anti-Malware Protection, Application Control thời hạn 1 năm
		Thiết bị có đầy đủ bản quyền sử dụng dịch vụ Sandbox Cloud từ nhà sản xuất thời hạn 1 năm
3.9	Bảo hành	Dịch vụ bảo hành phần cứng và hỗ trợ kỹ thuật của hãng sản xuất, thời hạn 1 năm
II.	**LICENSE**	
2.1	Bản quyền sử dụng	Thiết bị có đầy đủ bản quyền sử dụng các tính năng IPS, Anti-Malware Protection, Application Control thời hạn 1 năm
2.2		Thiết bị có đầy đủ bản quyền sử dụng dịch vụ Sandbox Cloud từ nhà sản xuất thời hạn 1 năm

III.	Module 10G SR SFP+ 10GBASE-SR SFP+ 850nm LC 300m (OM3), 400m (OM4) MMF, with DOM function, Commercial Temperature	4
IV.	Module 25G SR SFP28 25GBASE-SR SFP28 850nm LC Connectors, up to 70m(OM3) or 100m(OM4) on MMF, with DOM function	4
V.	Dây nhảy quang OM4, 15m	4
VI.	Dây nhảy quang OM4, 20m	4
B	**DỊCH VỤ TRIỂN KHAI HỆ THỐNG**	
1	Khảo sát	Khảo sát hiện trạng & chuẩn hóa môi trường: - Kiểm tra các kết nối, rule, zone,... của thiết bị Fortinet 600D hiện tại đang sử dụng. - Sao lưu cấu hình Fortinet 600D - Upgrade Firmware mới nhất cho thiết bị firewall mới.
2	Thiết kế	Thiết kế map cổng & cấu trúc interface trên thiết bị firewall mới: - Bảng ánh xạ: WAN, LAN/DMZ, LACP/aggregate, hardware-switch vs. interface độc lập - Tạo trước cấu trúc interface/switch/VLAN/aggregate/zone trên firewall mới:
3	Chuyển đổi cấu hình	Chuyển đổi cấu hình: - 300 rule firewall - 150 VIP - 11 interface - SD wan rule - 20 Static route - 5 policy route - 50 user VPN (local, ldap,radius) - 6 user groups - Config Log, monitor, SNMP, SSL VPN, VPN site to site,…

4	Chuyển hệ thống	Pre-staging & kiểm thử trước cắt chuyển: - Import cấu hình đã "massage" lên thiết bị firewall mới - Kiểm thử lab: parse policy, NAT/VIP, object, route, VPN profiles, UTM profiles; kiểm tra log tới FAZ/SIEM test
5	Quy trình thực hiện, các bước thực hiện, thời gian downtime	Cắt chuyển (Cutover): - Đảm bảo downtime tối thiểu (< 2 hours) - Kịch bản, checklist rõ ràng các bước thực hiện.
6	Kiểm thử, tinh chỉnh	Kiểm thử sau cắt chuyển & tinh chỉnh: - Routing nội bộ/Internet, NAT/VIP, IPsec/SSL-VPN, SD-WAN/health-check, UTM, quản trị/Local-in, logging FMG/FAZ/SIEM, NTP, AAA. - Hiệu năng: get system performance status, diagnose sys top, kiểm tra session/throughput. Rollback: - Trường hợp cutover không thành công, thực hiện rollback. - Biên bản sự cố