Phần 2. YÊU CẦU VỀ KỸ THUẬT
Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

I. Giới thiệu chung về dự án, gói thầu

1. Tên dự án và gói thầu

- Tên dự án: Đầu tư thay thế thiết bị tường lửa mạng giai đoạn 2.
- Tên gói thầu: Đầu tư thay thế thiết bị tường lửa mạng giai đoạn 2.

2. Mục tiêu đầu tư

- Thay thế các thiết bị tường lửa mạng tại phân vùng Internal, giám sát an ninh mạng tập trung và bảo mật cơ sở hạ tầng đã cũ, hết khấu hao, hết hạn bảo hành, bảo trì, hết vòng đời thiết bị, Hãng sản xuất không còn hỗ trợ và duy trì dòng sản phẩm tại Trung tâm dữ liệu PDC và BDC.
- Trang bị cặp thiết bị tường lửa mới tại hệ thống thông tin dự phòng thảm họa.
- Đảm bảo hoạt động an toàn, ổn định hệ thống mạng, triển khai các thiết bị tường lửa mạng để bảo vệ, phòng chống tấn công hệ thống mạng, máy chủ, ứng dụng, dữ liệu của Agribank. Nâng cao năng lực an ninh bảo mật và phù hợp với Đề án chiến lược phát triển CNTT giai đoạn 2022-2026, định hướng đến năm 2030.
- Tuân thủ các quy định về an toàn, bảo mật hệ thống thông tin trong hoạt động ngân hàng của Nhà nước, của Agribank.

3. Quy mô đầu tư

- Đầu tư các thiết bị tường lửa mạng mới để thay thế các thiết bị tường lửa mạng cũ tại phân vùng Internal, giám sát an ninh mạng tập trung và bảo mật cơ sở hạ tầng tại Trung tâm dữ liệu PDC, BDC, bao gồm:
  + Tường lửa mạng bảo vệ các hệ thống máy chủ chính tại PDC.
  + Tường lửa mạng bảo vệ các hệ thống máy chủ chính tại BDC.
  + Tường lửa mạng bảo vệ các hệ thống máy chủ tại DRC.
- Tổ chức triển khai và tích hợp các thiết bị tường lửa với hệ thống mạng, hệ thống quản trị tường lửa mạng hiện tại và các hệ thống liên quan khác của Agribank.
- Đào tạo và chuyển giao tài liệu.

4. Địa điểm đầu tư

Các thiết bị được triển khai tại các địa điểm sau:

- Trung tâm dữ liệu tại Tòa nhà C3, Phường Phương Liệt, TP Hà Nội.
- Trung tâm dữ liệu tại Khu đất A5 – THCT2, Khu đô thị mới Lê Trọng Tấn, xã An Khánh, TP Hà Nội.

5. Thời gian thực hiện gói thầu

Thời gian thực hiện hợp đồng gói thầu tối đa là 06 tháng (bao gồm cả ngày nghỉ, ngày lễ) kể từ ngày hợp đồng có hiệu lực.

II. Yêu cầu về kỹ thuật

1. Yêu cầu đối với giải pháp

- Đảm bảo an toàn, an ninh mạng, bảo vệ và phòng chống tấn công hệ thống mạng, máy chủ, ứng dụng, dữ liệu quan trọng của Agribank tại các Trung tâm dữ liệu.
- Thiết bị tường lửa mạng thay thế phải đảm bảo là các thiết bị tường lửa thế hệ mới, thuộc các dòng thiết bị chuyên dùng cho môi trường mạng doanh nghiệp lớn, phải nằm trong nhóm Leaders theo đánh giá "Enterprise Firewall Solutions" của công ty nghiên cứu thị trường Forrester (www.forrester.com) năm 2023 hoặc năm 2024, có độ tin cậy, tính sẵn sàng, tốc độ cao và năng lực xử lý số lượng kết nối đồng thời lớn đáp ứng các thời điểm giao dịch tăng đột biến hay đủ năng lực xử lý ngăn chặn, chống các hoạt động tấn công hệ thống mạng cường độ cao.
- Các thiết bị tường lửa mạng thay thế phải đảm bảo tương thích, tích hợp được hoàn toàn với hệ thống mạng, hệ thống tường lửa và hệ thống quản lý tường lửa tập trung các thiết bị tường lửa mạng phân vùng Internal, giám sát an ninh mạng tập trung của Agribank.
- Thiết kế an ninh bảo mật mạng đảm bảo kiến trúc bảo vệ mạng theo nhiều lớp và phân vùng mạng, hoàn toàn phù hợp với mô hình bảo mật Zero Trust (mô hình bảo mật tiêu chuẩn, toàn diện nhất hiện nay). Đồng thời giải pháp kỹ thuật phải đảm bảo tính sẵn sàng cao, các thiết bị tường lửa mạng cùng phân lớp, cùng chức năng phải dự phòng được cho nhau nhằm đảm bảo hoạt động liên tục của các ứng dụng, dịch vụ quan trọng.
- Thiết lập các chính sách an ninh theo quy định của Agribank về an toàn thông tin theo từng khu vực, Module, Zone. Đảm bảo ngăn chặn các truy cập không cho phép, sự xâm nhập của malware, virus, spyware, v.v… từ mạng ngoài vào trung tâm dữ liệu của Agribank.

2. Yêu cầu về kiến trúc tổng thể và chi tiết

2.1. Yêu cầu về kiến trúc tổng thể

a) Kiến trúc tổng thể giai đoạn 2 của dự án

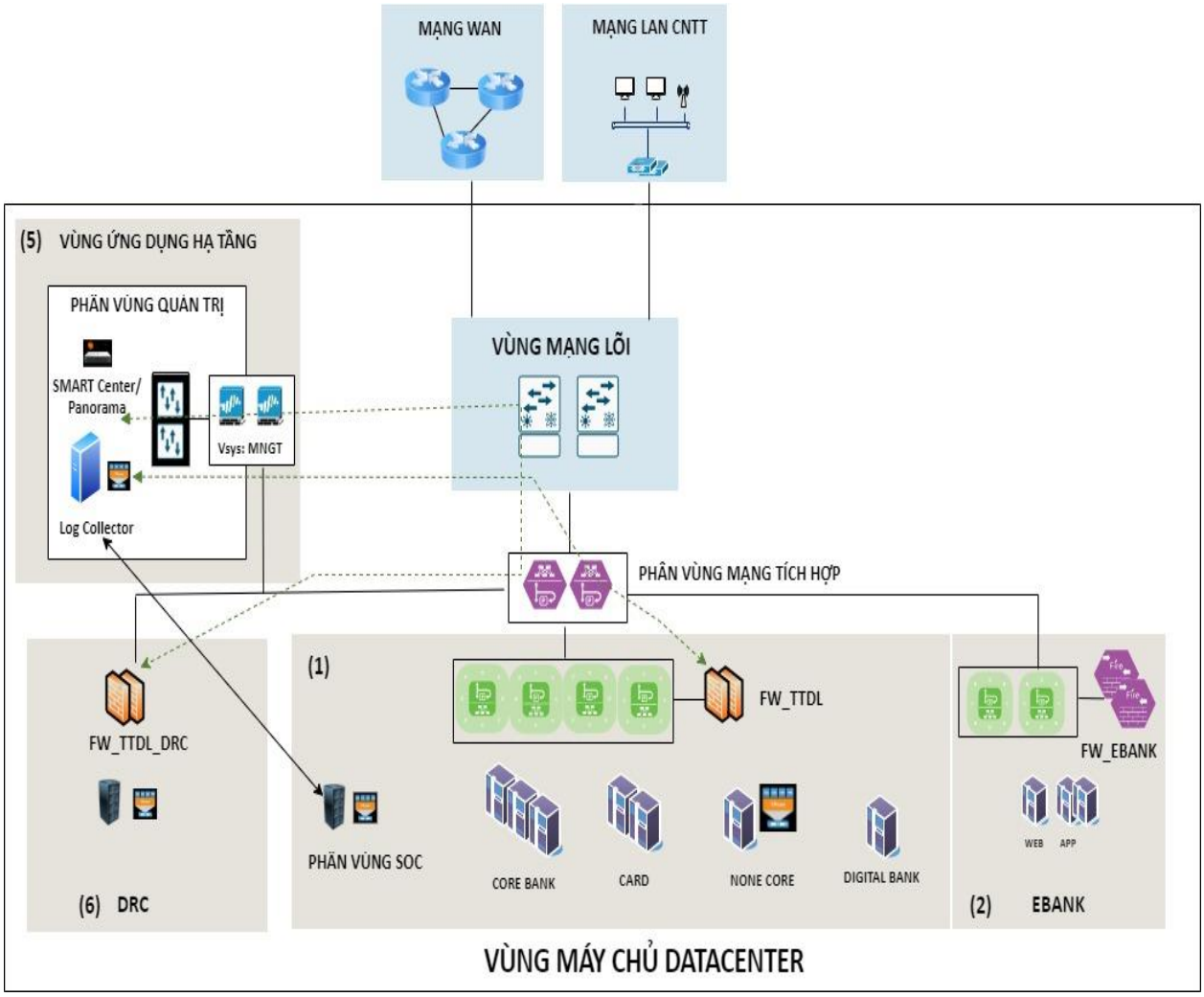
Đảm bảo mô hình 02 Trung tâm dữ liệu PDC và BDC của Agribank hoạt động song song và có thể dự phòng cho nhau thì mô hình phân vùng mạng, thiết bị tường lửa bảo vệ mạng mới tại 02 Trung tâm dữ liệu PDC và BDC giống nhau về kiến trúc và số lượng.

Đảm bảo hệ thống thông tin dự phòng thảm họa được bảo vệ tách biệt, kiểm soát truy cập về mặt logic với hệ thống chính nhằm giảm thiểu nguy cơ tấn công mạng leo thang vào các HTTT dự phòng.

Kiến trúc tường lửa bảo vệ mạng Agribank sau khi triển khai thay thế các thiết bị mới vẫn gồm 2 lớp chính: lớp ngoài bảo vệ các phân vùng mạng vành đai và hạ tầng phía ngoài; lớp trong bảo vệ các phân vùng mạng máy chủ, ứng dụng, dữ liệu trong phân vùng Intra DC tại Trung tâm dữ liệu PDC và BDC, các máy

chủ HTTT tại hệ thống thông tin dự phòng thảm họa. Kiến trúc hệ thống tường lửa tuân thủ mô hình bảo mật Zero Trust, bảo vệ theo chiều sâu và phân vùng. Mặt khác, áp dụng các công nghệ an ninh như: IPS, Antivirus, AntiBot, v.v… nhằm kiểm soát toàn bộ các lưu lượng vào ra hệ thống máy chủ chính, hệ thống máy chủ dự phòng và hệ thống giám sát an ninh mạng tập trung.

b) Hệ thống quản trị tập trung các thiết bị tường lửa mạng



- Sử dụng hệ thống quản lý tập trung các thiết bị tường lửa bảo vệ mạng lớp trong hiện tại của Agribank để quản lý, cung cấp giao diện quản trị đồng nhất theo thời gian thực các thiết bị tường lửa mới và thiết bị tường lửa đang sử dụng của Agribank. Ngoài ra, cho phép việc quản lý triển khai cấu hình, chính sách các thiết bị tường lửa mới một cách tập trung thống nhất, phân tích, điều tra và báo cáo về các sự cố về an ninh trên tổng thể hệ thống mạng lớp trong của Agribank. Hệ thống quản lý tập trung các thiết bị tường lửa mạng hiện có các tính năng chính sau:

+ Bảng điều khiển hợp nhất nhằm quản lý các yếu tố bảo mật từ chính sách đến ngăn chặn các mối đe dọa.

+ Có khả năng triển khai, quản lý tập trung các cấu hình, chính sách cho các

thiết bị tường lửa của hệ thống.

+ Có khả năng phân chia, quản trị người dùng quản trị theo các chính sách riêng phụ thuộc vào quyền hạn của từng người quản trị.

+ Cung cấp khả năng phân tích, điều tra và báo cáo mỗi khi có sự cố về an ninh cũng như sự thay đổi của người quản trị.

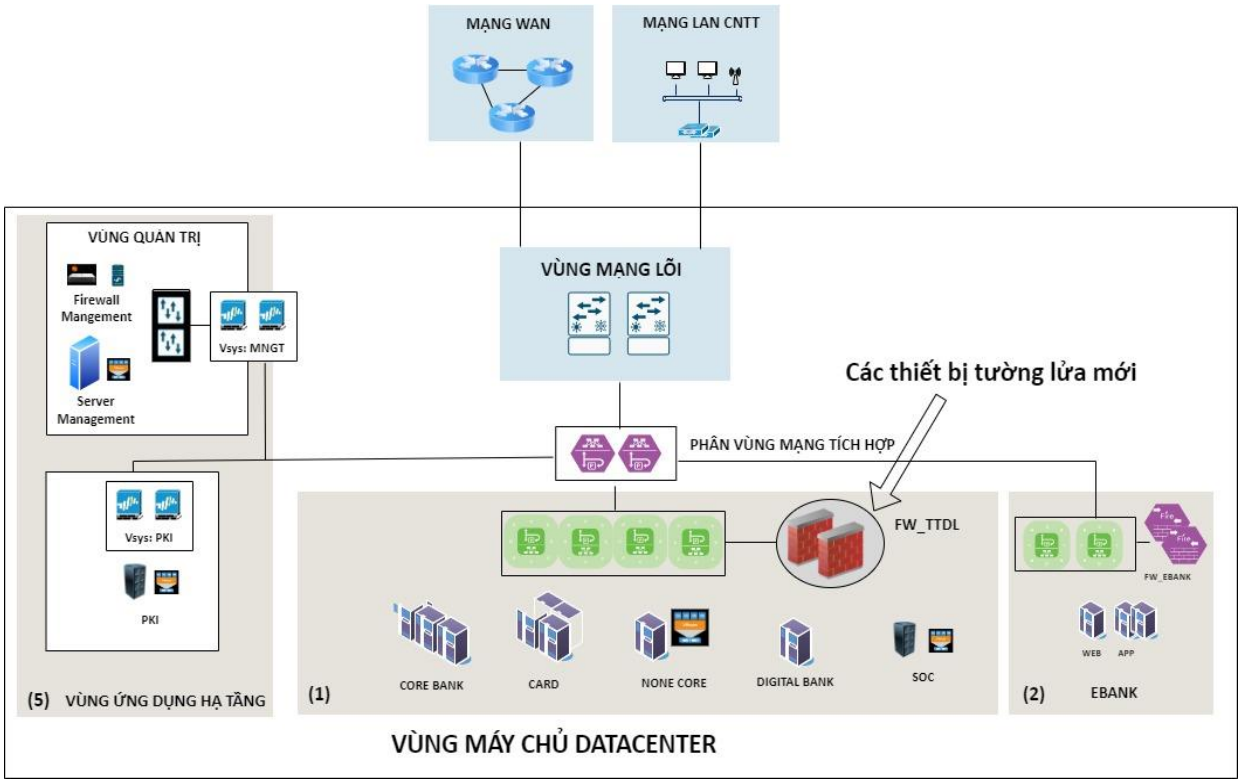
- Hiện tại hệ thống quản lý tập trung các tường lửa bảo vệ mạng lớp trong gồm có 02 thành phần chính, được cài đặt trên thiết bị chuyên dụng của Agribank, cụ thể như sau:

+ Smart Center/Panorama: quản trị tập trung tất cả các thiết bị tường lửa bảo vệ mạng lớp trong, bao gồm: chính sách, cấu hình, phân quyền quản trị, cập nhật (OS, signature AV, v.v…).

+ Log collector: thu thập logs từ tất cả thiết bị tường lửa, đồng thời đẩy logs về hệ thống giám sát an ninh mạng tập trung (SOC); tạo báo cáo dựa trên dữ liệu logs thu được.

2.2. Yêu cầu về kiến trúc chi tiết

a) Kiến trúc chi tiết tường lửa mạng bảo vệ lớp trong tại PDC và BDC:



Hệ thống tường lửa mạng lớp trong tại PDC và BDC bao gồm các phân vùng: Internal, giám sát an ninh mạng tập trung (SOC), PKI, E-banking. Trong đó bao gồm các máy chủ dữ liệu và các máy chủ ứng dụng như: các máy chủ ứng dụng IPCAS, máy chủ cơ sở dữ liệu IPCAS, các máy chủ hệ thống OSB, các máy chủ

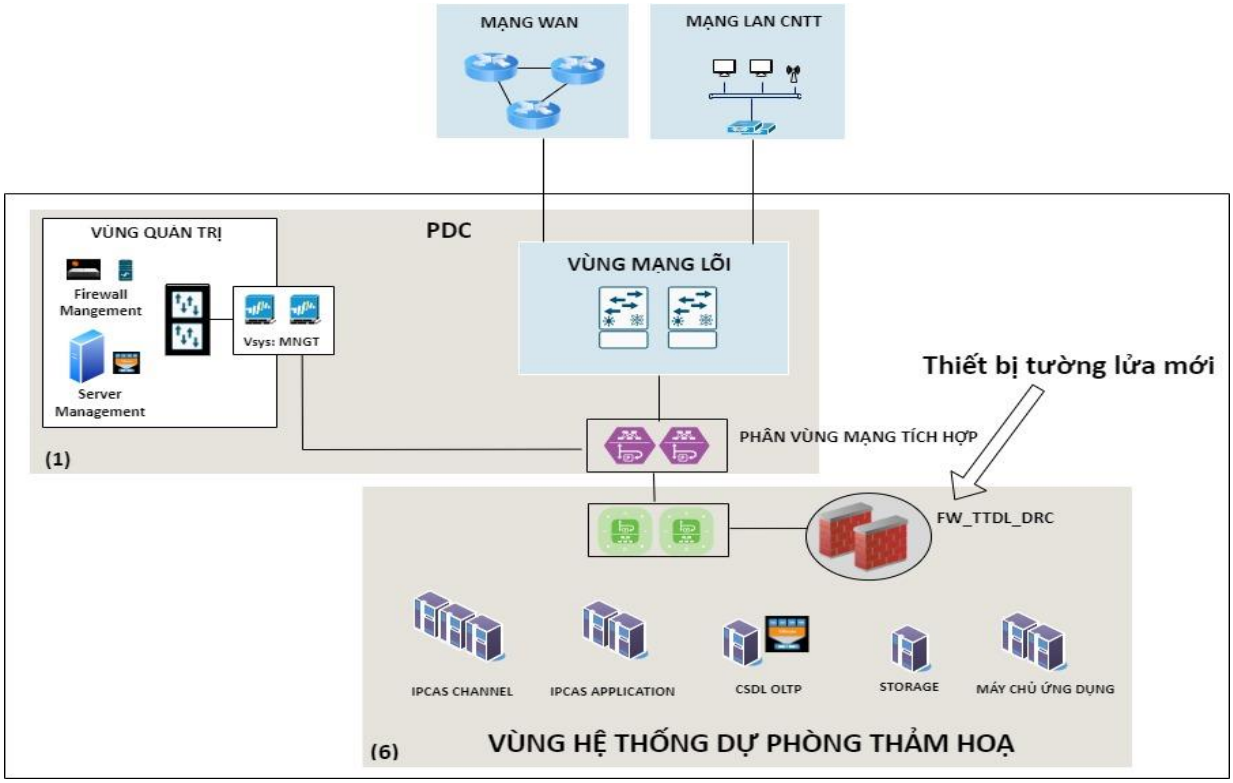
ứng dụng nghiệp vụ, các máy chủ dịch vụ Thẻ, các máy chủ kết nối thanh toán, v.v... Do tính chất đặc biệt quan trọng hệ thống máy chủ, dịch vụ tại IntraDC nên dự án sẽ trang bị các cặp thiết bị tường lửa thế hệ mới, chuyên dụng trong môi trường mạng doanh nghiệp, có năng lực xử lý lớn để bảo vệ và kiểm soát kết nối mạng cho các phân vùng Internal, hệ thống máy chủ chính với chính sách kiểm soát truy cập riêng cho từng phân vùng mạng.

Các thiết bị tường lửa mạng thế hệ mới với các công nghệ an ninh như: IPS, ngăn chặn virus, ngăn chặn mã độc nguy hiểm, v.v… nhằm kiểm soát toàn bộ các lưu lượng vào/ra hệ thống máy chủ, dịch vụ quan trọng, ngăn chặn các tấn công khai thác lỗ hổng trên giao thức mạng, hoặc lỗ hổng của hệ điều hành, của phần mềm để tấn công từ mạng ngoài.

Các thiết bị tường lửa mới sẽ được quản lý bởi hệ thống quản lý tập trung các tường lửa hiện tại của Agribank nhằm đảm bảo việc quản lý chính sách, cấu hình tập trung thống nhất; dễ dàng cho người quản trị trong quá trình phân tích, điều tra và báo cáo về các sự cố về an ninh mạng.

Các cặp tường lửa này sẽ hoạt động ở chế độ Active-Active hoặc Active-Passive, ở chế độ này cấu hình 2 thiết bị cũng như các phiên kết nối sẽ được đồng bộ tự động giữa 2 thiết bị tường lửa, giúp đảm bảo hoạt động của hệ thống, dịch vụ không bị gián đoạn. Cổng đồng bộ được thiết kế với 2 cổng vật lý riêng biệt, đảm bảo tính sẵn sàng và hạn chế các lỗi xảy ra.

b) Kiến trúc chi tiết tường lửa mạng bảo vệ các hệ thống máy chủ tại DRC



Hệ thống máy chủ tại DRC bao gồm các máy chủ vật lý, thiết bị (tủ đĩa, SAN Switch) để phục vụ khôi phục hệ thống khi xảy ra sự cố/thảm họa gây hậu quả

nghiêm trọng làm dừng hoạt động của HTTT. Trong đó bao gồm các máy chủ dữ liệu và các máy chủ ứng dụng, dịch vụ như: các máy chủ cơ sở dữ liệu, ứng dụng cho hệ thống IPCAS, hệ thống OSB; máy chủ cơ sở dữ liệu dự phòng None Core; máy chủ hệ thống AD/Email/Antivirus, v.v... Do tính chất đặc biệt quan trọng hệ thống máy chủ, ứng dụng, dịch vụ tại DRC nhằm sẵn sàng phục hồi nhanh HTTT khi hệ thống chính gặp sự cố, đưa hệ thống trở lại hoạt động bình thường theo yêu cầu nghiệp vụ nên dự án sẽ trang bị cặp thiết bị tường lửa thế hệ mới, chuyên dụng trong môi trường mạng doanh nghiệp, có năng lực xử lý cao để đảm bảo DRC được bảo vệ tách biệt. Kiểm soát kết nối mạng, kiểm soát truy cập về mặt logic với hệ thống chính nhằm giảm thiểu nguy cơ tấn công mạng leo thang vào các HTTT với chính sách kiểm soát truy cập riêng cho từng phân vùng mạng.

Các thiết bị tường lửa mạng thế hệ mới với các công nghệ an ninh như: IPS, ngăn chặn virus, ngăn chặn mã độc nguy hiểm, v.v… nhằm kiểm soát toàn bộ các lưu lượng vào/ra DRC, ngăn chặn các tấn công khai thác lỗ hổng trên giao thức mạng, hoặc lỗ hổng của hệ điều hành, của phần mềm.

Các cặp tường lửa này sẽ hoạt động ở chế độ Active-Active hoặc Active-Passive, ở chế độ này cấu hình 2 thiết bị cũng như các phiên kết nối sẽ được đồng bộ tự động giữa 2 thiết bị tường lửa, giúp đảm bảo hoạt động của hệ thống, dịch vụ không bị gián đoạn. Cổng đồng bộ được thiết kế với 2 cổng vật lý riêng biệt, đảm bảo tính sẵn sàng và hạn chế các lỗi xảy ra.

3. Yêu cầu kỹ thuật đối với thiết bị

3.1. Danh mục các thiết bị tường lửa mạng

STT	Thiết bị	Số lượng	Đơn vị
1	Thiết bị tường lửa mạng bảo vệ các hệ thống máy chủ chính tại PDC (FW_TTDL_PDC)	02	Bộ
2	Thiết bị tường lửa mạng bảo vệ các hệ thống máy chủ chính tại BDC (FW_TTDL_BDC)	02	Bộ
3	Thiết bị tường lửa mạng bảo vệ các hệ thống máy chủ tại DRC (FW_TTDL_DRC)	02	Bộ
Tổng số thiết bị tường lửa mạng		**06**	Bộ

3.2. Yêu cầu chung đối với các thiết bị

- Các thiết bị tường lửa phải của chính hãng sản xuất, mới 100%, được sản xuất tối đa không quá 06 tháng trước ngày ký hợp đồng. Các thiết bị phải có đầy đủ các giấy tờ chứng minh gồm: Giấy chứng nhận chất lượng hàng hóa của hãng sản xuất (CQ); giấy xác nhận bảo hành, hỗ trợ kỹ thuật của hãng sản xuất; các giấy tờ chứng minh nguồn gốc xuất xứ của hàng hóa, vận đơn (bill of lading), phiếu đóng gói hàng hóa (packing list).

- Yêu cầu về thời gian sản xuất thiết bị và vòng đời sản phẩm: Các thiết bị tường lửa chưa có thông báo của hãng về việc thay thế, chưa có thông báo dừng sản xuất hoặc/và dừng hỗ trợ sản phẩm từ phía nhà sản xuất, tính đến thời điểm nộp Hồ sơ dự thầu.

- Các thiết bị tường lửa phần cứng phải có đầy đủ phụ kiện đi kèm thiết bị cùng các tài liệu kỹ thuật về thiết bị của hãng sản xuất như: Các catalogue hoặc địa chỉ các Website của Hãng sản xuất giới thiệu về công nghệ tính năng kỹ thuật của thiết bị.

3.3. Thiết bị tường lửa mạng bảo vệ các hệ thống máy chủ chính tại PDC (FW_TTDL_PDC)

a) Thiết bị tường lửa mạng và transceiver

STT	Nội dung	Yêu cầu kỹ thuật tối thiểu hoặc tương đương
1	Interfaces	- 04 x 10/25GbE SFP28 ports - 04 x 40/100GbE QSFP+/QSFP28 ports - Management port
2	Transceiver	- 04 x 25GBASE-SR SFP28 - 04 x 40GBASE-SR QSFP+/QSFP28
3	Storage Capacity	≥ 480 GB SSD
4	Threat Prevention Throughput	≥ 24 Gbps
5	Concurrent Sessions /Connections	≥ 5.000.000
6	New Sessions/Second or New Connections/Second	≥ 780.000
7	Routing	Static routes, OSPF, BGP, RIP, Policy-based routing/forwarding
8	Management	- Centralized Management - SSH, HTTPS, SNMP
9	High Availability	Active-Active, Active-Passive
10	Virtual Domains / Virtual Systems /Virtual Contexts (included license)	≥ 5
11	Power Supplies	- Dual power supply - 200V to 240V AC, 50Hz – 60Hz - 02 x Patch Cord C13-14

b) Bản quyền phần mềm (Subscription)

Bản quyền cho thiết bị tường lửa mạng tại PDC, thời gian tối thiểu 03 năm kể từ ngày nghiệm thu hợp đồng, bao gồm các tính năng sau:

- App ID/Application Control.
- Threat Prevention: IPS, Antivirus, AntiBot/Antispyware.
- DNS Trap/Sinkholing.

3.4. Thiết bị tường lửa mạng bảo vệ các hệ thống máy chủ chính tại BDC (FW_TTDL_BDC)

a) Thiết bị tường lửa mạng và transceiver

STT	Nội dung	Yêu cầu kỹ thuật tối thiểu hoặc tương đương
1	Interfaces	- 04 x 10/25GbE SFP28 ports - 02 x 40/100GbE QSFP+/QSFP28 ports - Management port
2	Transceiver	- 04 x 25GBASE-SR SFP28 - 02 x 40GBASE-SR QSFP+/QSFP28
3	Storage Capacity	≥ 480 GB SSD
4	Threat Prevention Throughput	≥ 19,2 Gbps
5	Concurrent Sessions /Connections	≥ 3.000.000
6	New Sessions/Second or New Connections/Second	≥ 624.000
7	Routing	Static routes, OSPF, BGP, RIP, Policy-based routing/forwarding
8	Management	- Centralized Management - SSH, HTTPS, SNMP
9	High Availability	Active-Active, Active-Passive
10	Virtual Domains / Virtual Systems /Virtual Contexts (included license)	≥ 5
11	Power Supplies	- Dual power supply - 200V to 240V AC, 50Hz – 60Hz - 02 x Patch Cord C13-14

b) Bản quyền phần mềm (Subscription)

Bản quyền cho thiết bị tường lửa mạng tại BDC, thời gian tối thiểu 03 năm kể từ ngày nghiệm thu hợp đồng, bao gồm các tính năng sau:

- App ID/Application Control.
- Threat Prevention: IPS, Antivirus, AntiBot/Antispyware.
- DNS Trap/Sinkholing.

3.5. Thiết bị tường lửa mạng bảo vệ các hệ thống máy chủ tại DRC (FW_TTDL_DRC)

a) Thiết bị tường lửa mạng và transceiver

STT	Nội dung	Yêu cầu kỹ thuật tối thiểu hoặc tương đương
1	Interfaces	- 04 x 10/25GbE SFP28 ports - 02 x 40/100GbE QSFP+/QSFP28 ports - Management port
2	Transceiver	- 04 x 25GBASE-SR SFP28 - 02 x 40GBASE-SR QSFP+/QSFP28
3	Storage Capacity	≥ 480 GB SSD
4	Threat Prevention Throughput	≥ 12 Gbps
5	Concurrent Sessions /Connections	≥ 3.000.000
6	New Sessions/Second or New Connections/Second	≥ 390.000
7	Routing	Static routes, OSPF, BGP, RIP, Policy-based routing/forwarding
8	Management	- Centralized Management - SSH, HTTPS, SNMP
9	High Availability	Active-Active, Active-Passive
10	Virtual Domains / Virtual Systems /Virtual Contexts (included license)	≥ 2
11	Power Supplies	- Dual power supply - 200V to 240V AC, 50Hz – 60Hz - 02 x Patch Cord C13-14

b) Bản quyền phần mềm (Subscription)

Bản quyền cho thiết bị tường lửa mạng tại DRC, thời gian tối thiểu 03 năm kể từ ngày nghiệm thu hợp đồng, bao gồm các tính năng sau:

- App ID/Application Control.
- Threat Prevention: IPS, Antivirus, AntiBot/Antispyware.
- DNS Trap/Sinkholing.

4. Yêu cầu tổ chức triển khai, bảo hành và hỗ trợ xử lý kỹ thuật

4.1. Yêu cầu chung

Nhà thầu phải xây dựng phương pháp triển khai bao gồm các nội dung:

- Lập bảng tiến độ thực hiện hoặc kế hoạch thực hiện.
- Lập nhật ký công tác triển khai.
- Tổ chức triển khai, bao gồm:

+ Khảo sát, kiểm tra, kiểm thử, bàn giao và nghiệm thu thiết bị, lắp đặt.

+ Triển khai giải pháp.
+ Tích hợp.
+ Đánh giá, hiệu chỉnh và tối ưu hoạt động.

- Nhà thầu chịu trách nhiệm vận chuyển thiết bị đến địa điểm kiểm tra, kiểm thử, bàn giao và nghiệm thu tại Trung tâm Công nghệ thông tin – Khu đất A5 – THCT2, Khu đô thị mới Lê Trọng Tấn, xã An Khánh, TP Hà Nội. Sau khi hoàn thành việc kiểm tra, kiểm thử, Nhà thầu chịu trách nhiệm vận chuyển thiết bị đến các địa điểm triển khai.
- Việc triển khai, tích hợp các thiết bị tường lửa phải không làm ảnh hưởng đến các dịch vụ của Agribank cung cấp cho khách hàng trong giờ giao dịch và đảm bảo tương thích, tích hợp được hoàn toàn với hệ thống mạng, hệ thống tường lửa và hệ thống quản lý tập trung các thiết bị tường lửa mạng hiện tại của Agribank.
- Nhà thầu chịu trách nhiệm thực hiện và các chi phí phát sinh khác (nếu có) trong việc triển khai các thiết bị tường lửa vào hệ thống Agribank (bao gồm cả việc phải nâng cấp, đồng bộ phần mềm hệ thống quản lý tập trung các thiết bị tường lửa mạng (nếu cần thiết) và chi phí các vật tư cần thiết để triển khai như: Cáp quang, cáp nhảy quang, cáp mạng, dây nhảy mạng, dây nguồn thiết bị, dây điện, dụng cụ mạng, các vật tư và phụ kiện khác, v.v...).

4.2. Yêu cầu các hạng mục công việc về triển khai

Nhà thầu chịu trách nhiệm thực hiện các hạng mục công việc sau:

a) Khảo sát, kiểm tra, kiểm thử, bàn giao và nghiệm thu thiết bị, lắp đặt:

- Khảo sát, kiểm tra các điều kiện để triển khai, đánh giá hiện trạng kiến trúc vật lý, logic và chính sách an ninh mạng các phân vùng;
- Lịch trình cung cấp, kiểm tra, kiểm thử, bàn giao và nghiệm thu thiết bị.
- Số lượng và nhiệm vụ của các cán bộ triển khai.
- Kiểm tra số lượng, chủng loại, hình thức vật lý bên ngoài của thiết bị.
- Kiểm tra giấy chứng nhận chất lượng và giấy tờ chứng minh nguồn gốc xuất xứ.
- Kiểm tra các thông số kỹ thuật, kiểm thử tính năng thiết bị, hoặc vận hành thử (nếu cần thiết), lập báo cáo.
- Các thiết bị sau khi kiểm tra, kiểm thử đáp ứng các yêu cầu theo hợp đồng sẽ được nghiệm thu, bàn giao để đưa vào sử dụng.
- Lắp đặt các thiết bị tường lửa mạng tại địa điểm triển khai.

b) Triển khai giải pháp:

Lập phương án triển khai chi tiết, phương án triển khai phải được chấp thuận của Agribank; triển khai cấu hình, chính sách an ninh mạng cho các thiết bị tường lửa mạng, bao gồm các hạng mục sau:

- Nâng cấp hệ điều hành, phần mềm an ninh lên phiên bản mới nhất được

chính hãng khuyến cáo;

- Triển khai giải pháp bảo mật tại PDC.
- Triển khai giải pháp bảo mật tại BDC.
- Triển khai giải pháp bảo mật tại DRC.

c) Tích hợp:

- Tích hợp với hệ thống mạng, thiết bị an ninh tại PDC.
- Tích hợp với hệ thống mạng, thiết bị an ninh tại BDC.
- Tích hợp với hệ thống mạng, thiết bị an ninh tại DRC.
- Tích hợp các thiết bị tường lửa mạng với hệ thống quản lý các thiết bị tường lửa mạng bảo vệ mạng lớp trong hiện tại của Agribank (quản lý cấu hình, chính sách an ninh, log, giám sát, phân tích tập trung).
- Tích hợp với hệ thống điều hành an ninh tập trung SOC của Agribank.

d) Đánh giá, hiệu chỉnh và tối ưu hoạt động:

- Xây dựng và thiết lập các chính sách an ninh theo từng nhóm ứng dụng, dịch vụ, máy chủ, v.v...
- Đánh giá, hiệu chỉnh, tối ưu hoạt động, cấu hình, chính sách an ninh mạng của hệ thống tường lửa nhằm bảo vệ an toàn, bảo mật các hệ thống máy chủ, ứng dụng, dữ liệu, người dùng, khách hàng và đối tác của Agribank.
- Nghiệm thu hệ thống đưa vào sử dụng sau khi hoàn thành đầy đủ các hạng mục công việc về khối lượng, chất lượng, tiến độ.

4.3. Yêu cầu bảo hành và hỗ trợ xử lý kỹ thuật

Trong thời gian bảo hành các thiết bị tường lửa mạng phải có quyền cập nhật các dấu hiệu tấn công (signature), mối đe dọa an ninh mới nhất và cập nhật các phiên bản hệ điều hành, phần mềm an ninh, các bản nâng cấp, các bản vá theo tiêu chuẩn của nhà sản xuất và đảm bảo các yêu cầu sau:

a) Các công việc bảo hành và hỗ trợ xử lý kỹ thuật

- Nhà thầu phải cung cấp dịch vụ bảo hành và hỗ trợ kỹ thuật của chính hãng sản xuất.
- Nhà thầu phải tổ chức bảo hành, hỗ trợ kỹ thuật và xử lý sự cố trong suốt thời gian bảo hành. Nhà thầu phải có phương án linh kiện, thiết bị cho việc thay thế, sửa chữa khắc phục sự cố trong thời gian bảo hành, trường hợp các linh kiện, thiết bị phần cứng bị hỏng không khắc phục được ngay mà phải chuyển về hãng sản xuất thì Nhà thầu chịu trách nhiệm thay thế thiết bị khác tương đương trong suốt quá trình sửa chữa, bảo hành để đảm bảo hệ thống an ninh mạng của Agribank không bị gián đoạn.
- Trường hợp phải thay thế thì các linh kiện, thiết bị phần cứng phải đảm bảo của chính hãng sản xuất, mới 100% hoặc tương đương về chủng loại, thông số kỹ thuật, hoạt động tốt và tương thích với hệ thống đang sử dụng. Nhà thầu phải đảm bảo Agribank không phải trả thêm bất kỳ một khoản chi phí nào khác

đối với thiết bị, vật tư thay thế trong suốt thời gian bảo hành.

- Khi có yêu cầu của Agribank, Nhà thầu phải thực hiện việc cập nhật các phiên bản hệ điều hành, các bản nâng cấp, các bản vá và mẫu tấn công, mối đe dọa an ninh mới nhất theo tiêu chuẩn của nhà sản xuất trong thời gian bảo hành và hỗ trợ kỹ thuật.

- Agribank được cấp tài khoản (nếu có) trên trang của chính hãng để mở case hỗ trợ xử lý kỹ thuật đảm bảo việc xử lý sự cố nhanh chóng và kịp thời.

- Nhà thầu phải đề xuất phương án tổ chức bảo hành, hỗ trợ xử lý lỗi của hệ thống đáp ứng các yêu cầu của Agribank, trong đó phải đảm bảo:

+ Cung cấp đầu mối liên lạc, tiếp nhận thông tin về bảo hãnh, hỗ trợ xử lý lỗi/sự cố đáp ứng yêu cầu 24x7 qua điện thoại, email hoặc kênh liên hệ hỗ trợ của hãng sản xuất.

+ Thời gian đáp ứng xử lý sự cố:

Cấp độ sự cố	**Mô tả**	**Thời gian đáp ứng**	**Phương thức hỗ trợ**
Rất cao; Cao	- Sự cố liên quan đến phần cứng hoặc hệ điều hành làm cho thiết bị không hoạt động được bình thường với đầy đủ công suất/hiệu năng. - Đối với các sự cố về an ninh mạng, Nhà thầu phải yêu cầu chuyên gia của chính hãng phối hợp khắc phục và xử lý.	Trong vòng 02 giờ kể từ khi nhận được thông báo của Agribank.	Tại chỗ 24x7: Nhà thầu phải cử cán bộ đến xử lý tại chỗ và phải đưa ra được phương án xử lý.
Trung bình; Thấp	Sự cố liên quan đến phần cứng hoặc hệ điều hành nhưng chưa ảnh hưởng ngay đến khả năng hoạt động bình thường với đầy đủ công suất của hệ thống.	Trong vòng 04 giờ kể từ khi nhận được thông báo của Agribank.	Hỗ trợ từ xa hoặc tại chỗ: Nhà thầu hỗ trợ từ xa để tìm ra nguyên nhân gây ra sự cố. Nếu việc xử lý từ xa không được, phải cử cán bộ đến xử lý tại chỗ, đưa ra được phương án xử lý.

b) Thời gian và địa điểm bảo hành

- Thời gian bảo hành: Tất cả các thiết bị phần cứng, phần mềm, dịch vụ hỗ trợ kỹ thuật được bảo hành tối thiểu 03 (ba) năm theo tiêu chuẩn chính hãng sản xuất kể từ ngày nghiệm thu hợp đồng.

- Địa điểm bảo hành và hỗ trợ: Các thiết bị được bảo hành tại địa điểm lắp đặt thiết bị.

5. Yêu cầu về đào tạo và chuyển giao tài liệu

5.1. Yêu cầu về đào tạo

Nhà thầu tổ chức khóa đào tạo hướng dẫn sử dụng; hướng dẫn vận hành, quản trị, cấu hình nâng cao các thiết bị tường lửa mạng cho các cán bộ kỹ thuật của Agribank với các yêu cầu như sau:

- Nội dung đào tạo:

+ Các tính năng nổi bật, được cập nhật trên thiết bị tường lửa thế hệ mới nhằm tăng cường kiểm soát truy cập mạng cũng như hỗ trợ phát hiện, ngăn chặn các mối đe doạ trên hệ thống mạng.

+ Thực hành cấu hình tạo cặp các firewall (gateway cluster).

+ Thực hành cấu hình tạo danh sách động.

+ Thực hành cấu hình tuỳ biến các cơ chế bảo mật; kiểm tra tuân thủ cấu hình so với các tiêu chuẩn khuyến nghị.

+ Khai thác, sử dụng các API hỗ trợ bởi giải pháp giúp tự động hoá công tác quản trị, vận hành hệ thống tường lửa.

+ Hiệu chỉnh, tối ưu hoạt động hệ thống tường lửa.

- Thời gian học: 05 ngày (tối thiểu 05 nội dung khác nhau).
- Số lượng: Tối thiểu 03 cán bộ.
- Giảng viên đào tạo có chứng chỉ của chính hãng và giảng viên trợ giảng hỗ trợ cho giảng viên đào tạo.
- Phương pháp đào tạo: Đào tạo trực tiếp.
- Địa điểm đào tạo: Do Nhà thầu đề xuất.
- Môi trường đào tạo: Môi trường đào tạo của chính hãng hoặc được chính hãng ủy quyền, đảm bảo đầy đủ cơ sở vật chất, trang thiết bị, tài liệu cho đào tạo và đảm bảo chất lượng.

5.2. Yêu cầu về chuyển giao tài liệu

- Chuyển giao đầy đủ tài liệu:

+ Tài liệu khảo sát; tài liệu phương án triển khai chi tiết.

+ Hướng dẫn cài đặt, cấu hình, quản trị và vận hành hệ thống và thiết bị.

- Chuyển giao tài khoản quản trị:

+ Các tài khoản quản trị để đăng nhập hệ thống (như Root của OS, Administrator của thiết bị, tài khoản (nếu có) trên trang của chính hãng, v.v…) phải được bàn giao đầy đủ cho Agribank.

6. Yêu cầu dự kiến chi phí bảo trì

Dự kiến chi phí bảo trì và hỗ trợ kỹ thuật sau khi hết thời gian bảo hành (được tính bằng giá trị đầu tư/năm) bao gồm:

- Đối với thiết bị phần cứng tối đa từ 20%-25% chi phí thiết bị.
- Bản quyền/quyền sử dụng phần mềm (Subscription).

Nhà thầu giải pháp phải thực hiện cung cấp báo giá chi phí bảo trì trong thời gian 05 năm (có tách chi phí theo từng năm, từng hạng mục hàng hóa) kể từ thời

điểm hết hạn bảo hành theo quy định của hợp đồng.

Mục 2. Bản vẽ

Không có bản vẽ

Mục 3. Kiểm tra và thử nghiệm

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

- Kiểm tra trực tiếp trên thiết bị, qua catalogue, qua giao diện quản trị của thiết bị và các kịch bản thử nghiệm khác để đảm bảo hàng hóa có cấu hình và tính năng đáp ứng yêu cầu trong E-HSMT và E-HSDT.

- Kiểm tra giấy tờ chứng nhận xuất xứ của các thiết bị tường lửa mạng; giấy tờ chứng nhận/thư cam kết chất lượng của hãng sản xuất đối với các thiết bị tường lửa mạng và transceiver.

- Bất kỳ hàng hoá nào qua kiểm tra và thử nghiệm mà không phù hợp với đặc tính kỹ thuật theo hợp đồng thì Chủ đầu tư có quyền từ chối và Nhà thầu phải có trách nhiệm thay thế bằng hàng hoá khác hoặc tiến hành những điều chỉnh cần thiết để đáp ứng đúng các yêu cầu về đặc tính kỹ thuật. Trong trường hợp Nhà thầu không có khả năng thay thế hay điều chỉnh các hàng hoá không phù hợp, Chủ đầu tư có quyền đơn phương chấm dứt hợp đồng và mọi rủi ro, chi phí liên quan do Nhà thầu chịu.

- Các chi phí liên quan (nếu có) đến việc kiểm tra, thử nghiệm hàng hóa do Nhà thầu chịu trách nhiệm chi trả.