CHI TIẾT KỸ THUẬT HÀNG HOÁ

TT	Tên hàng hóa, thiết bị	Ký mã hiệu hàng hóa, thiết bị	Yêu cầu kỹ thuật
01	Gia hạn dịch vụ bảo trì, bảo hành thiết bị (phần cứng) và cập nhật phần mềm hệ thống của thiết bị tường lửa imperva X2520 Web Application Firewall	Imperva X2520	- Gia hạn thời hạn bảo hành, bảo trì 12 tháng - Gia hạn bảo hành thiết bị tường lửa Imperva từ chính hãng sản xuất hoặc nhà cung cấp chính thức được ủy quyền. - Thiết bị hỏng sẽ được sửa chữa miễn phí, trong quá trình sửa chữa sẽ có thiết bị khác thay thế để duy trì hệ thống chạy xuyên suốt thời gian bảo hành - Định kỳ kiểm tra thiết bị bằng phương pháp truy cập online kiểm tra lỗi thiết bị và hệ thống.
			Yêu cầu chung: - Gia hạn phần mềm hệ thống của 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. Yêu cầu chi tiết: - 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: Cross-Site Scripting (XSS) Broken Authentication and Session Management Insecure Direct Object References Cross-Site Request Forgery (CSRF) Security Misconfiguration Insecure Cryptographic Storage

TT	Tên hàng hóa, thiết bị	Ký mã hiệu hàng hóa, thiết bị	Yêu cầu kỹ thuật
			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, scripts based trên Web browser + Cung cấp chính sách an ninh site scraping, Application DDoS, 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

TT	Tên hàng hóa, thiết bị	Ký mã hiệu hàng hóa, thiết bị	Yêu cầu kỹ thuật
			(malicious encoding, HTTP protocol violations, application profile 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) + Real-time dashboard
02	Gia hạn sử dụng hệ thống phần mềm quản trị tập trung VM150	VM150	- Hãng sản xuất: Imperva. - Chủng loại: VM150. - Phần mềm hệ thống quản trị tập trung giúp bảo đảm việc quản lý và giám sát hoạt động các thiết bị hiệu quả nhất theo cơ chế thống nhất. - Phương thức cung cấp: Cấp tài khoản gia hạn truy cập hệ thống phần mềm sử dụng và quản lý thiết bị Imperva trên VM150. - Thời hạn sử dụng, bản quyền: 12 tháng, hỗ trợ kỹ thuật 24/7. - Tính năng và thông số kỹ thuật: + 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.

TT	Tên hàng hóa, thiết bị	Ký mã hiệu hàng hóa, thiết bị	Yêu cầu kỹ thuật
			+ 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
03	Cập nhật phần mềm và gia hạn bản quyền thiết bị tường lửa Sophos SG210	Sophos SG210	Yêu cầu chung: - Cập nhật và gia hạn bản quyền phần mềm tường lửa Sophos SG210 từ chính hãng sản xuất hoặc nhà cung cấp chính thức được ủy quyền. - Thời hạn sử dụng, bản quyền: 06 tháng, hỗ trợ kỹ thuật 24/7. - Thiết bị sau khi được gia hạn bản quyền và cập nhật phần mềm có thể tiếp tục sử dụng ngay, không yêu cầu cài đặt hoặc hiệu chỉnh lại các tham số hệ thống. Yêu cầu chi tiết: - Cập nhật phiên bản: Gia hạn bảo hành thiết bị 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: + Phát hiện và ngăn chặn các cuộc tấn công mạng qua tính năng IPS với hơn 18.000 mẫu tấn công. + Chống tấn công DoS và một phần DDoS + Cho phép ngăn chặn theo dải IP từ các quốc gia cụ thể + Kiểm soát các giao tiếp không an toàn: FTP, IRC, PPTP, TFTP. * Advanced Threat Protection

TT	Tên hàng hóa, thiết bị	Ký mã hiệu hàng hóa, thiết bị	Yêu cầu kỹ thuật
			+ Phát hiện và ngăn chặn các giao tiếp cố gắng kết nối và kiểm soát máy chủ qua DNS, AFC, HTTP Proxy và firewall. + Phát hiện các máy tính bị nhiễm mã độc trong mạng cố gắng giao tiếp ra bên ngoài. * Web Protection: + Dữ liệu hơn 35 triệu website cho vào các nhóm khác nhau để có thể dễ dàng ngăn chặn người dùng truy cập tới những website theo nhóm cụ thể. + Application Control: Cơ sở dữ liệu về các ứng dụng chạy trên nền web cho phép người quản trị dễ dàng quản lý và ngăn chặn các dịch vụ không an toàn và gây ảnh hưởng hệ thống mạng. + 2 Engine phát hiện mã độc bảo vệ người dùng khi truy cập web. + Chống lại các tấn công tới người dùng từ các website. + Thiết lập các chính sách truy cập web. * Email Protection: + Ngăn chặn spam mail và các loại mã độc lây nhiễm qua Email. * VPN: + Hỗ trợ các giao thức VPN: SSL, IPsec, AES, PFS, RSA, X509. * Web Application Firewall Protection: + Bảo vệ hệ thống Web server thông qua các tính năng: Reverse proxy, URL hardening, Form hardening, SQL Injection, XSS, Dual Anti-Virus.