NGÂN HÀNG NHÀ NƯỚC
VIỆT NAM
TRUNG TÂM THÔNG TIN TÍN DỤNG QUỐC GIA VIỆT NAM

Số: 1106 /TTTD-QLĐT
V/v mời báo giá hệ thống kiểm soát truy cập cho mạng LAN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 12 tháng 08 năm 2025

Kính gửi:

Trung tâm Thông tin tín dụng Quốc gia Việt Nam (CIC) có nhu cầu mua hệ thống kiểm soát truy cập Network Access Control cho mạng LAN (NAC). CIC mời Quý đơn vị cung cấp báo giá đối với hàng hóa nói trên, yêu cầu kỹ thuật chi tiết gửi kèm công văn này.

Đề nghị Quý đơn vị gửi báo giá về Trung tâm Thông tin tín dụng Quốc gia Việt Nam (Địa chỉ: số 45 Lý Thường Kiệt, phường Cửa Nam, Hà Nội) đồng thời gửi bản mềm về địa chỉ email: **qldt@creditinfo.org.vn, phongketoan@creditinfo.org.vn**. Báo giá của Quý đơn vị là cơ sở để CIC xây dựng dự toán và thực hiện thủ tục đấu thầu theo đúng quy định hiện hành.

Thời hạn gửi báo giá: chậm nhất ngày 25/08/2025.

Xin trân trọng cảm ơn./.

Nơi nhận:
- Như trên;
- P.NCPT (để đăng tải Website CIC);
- P.TCKT (để đăng Báo đấu thầu, thẩm định giá);
- Lưu VT, QLĐT.NNQHoa.

Gửi kèm:
- Yêu cầu kỹ thuật của hàng hóa.

KT. TỔNG GIÁM ĐỐC
PHÓ TỔNG GIÁM ĐỐC

TRUNG TÂM THÔNG TIN TÍN DỤNG QUỐC GIA VIỆT NAM

Phan Huy Thắng

PHỤ LỤC

(Kèm theo công văn mời báo giá số 1106 /TTTD-QLĐT ngày 12 /08/2025)

Hệ thống kiểm soát truy cập Network Access Control cho mạng LAN (NAC)

Nội dung	Yêu cầu kỹ thuật
Hệ thống kiểm soát truy cập Network Access Control cho mạng LAN (NAC)	
Khả năng quản trị thiết bị đầu cuối của toàn bộ hệ thống	>= 600 Thiết bị
Giải pháp quản trị tập trung NAC đặt tại Trung tâm dữ liệu Fornix	- Giải pháp có thể là phần cứng vật lý hoặc ảo hóa đáp ứng cài đặt trên nền tảng VMWARE 6.7. - Sử dụng để quản trị tập trung chính sách các thiết bị NAC tại trụ sở chính tại Hà Nội và chi nhánh Hồ Chí Minh. - Đảm bảo bản quyền đủ khả năng quản lý tối thiểu 600 thiết bị đầu cuối.
Thiết bị tại trụ sở chính	- Thiết bị NAC là phần cứng vật lý, tối thiểu 02 thiết bị, đảm bảo dự phòng HA. - Quản trị >=500 thiết bị đầu cuối. - Yêu cầu thiết bị như sau: • Dạng rackmount • Nguồn: >=2, đảm bảo dự phòng. • Số lượng cổng đồng 1Gbps: >=4. • Số lượng cổng quang 10Gbps đã bao gồm Module đi kèm: >= 2.
Giải pháp NAC tại chi nhánh Hồ Chí Minh	- Giải pháp NAC là phần cứng vật lý hoặc máy chủ vật lý (server) cài ảo hóa, có đảm bảo dự phòng HA (1+1) hoặc clustering. - Nếu sử dụng server, nhà thầu trang bị server kèm các phần mềm cần thiết có bản quyền, đang trong hạn hỗ trợ của nhà sản xuất. Yêu cầu đối với OS (nếu có) cài đặt trên hệ điều hành Windows (từ bản Windows server 2022 trở lên), Linux (Redhat 9.0 hoặc Ubuntu 22.04 trở lên). - Quản trị >=100 thiết bị đầu cuối. - Yêu cầu thiết bị như sau: • Dạng rackmount • Nguồn: >=2, đảm bảo dự phòng.

Nội dung	Yêu cầu kỹ thuật
	• Số lượng cổng đồng 1Gbps: >=4.
Tính năng quản lý và giám sát các thiết bị trong hệ thống mạng	- Giải pháp phải có khả năng khám phá và theo dõi không cần cài đặt agent cho tất cả các thiết bị ngay sau khi chúng kết nối vào mạng. - Phân loại các thiết bị thành các nhóm khác nhau: các thiết bị truyền thống (Windows, Linux, MacOS,…), các thiết bị kết nối phi truyền thống (camera IP, máy in, điện thoại, cảm biến, thiết bị tự động hóa tòa nhà v.v.). - Giải pháp phải hiển thị thông tin liên quan đến các thiết bị đầu cuối được kết nối với mạng như: IP Address, MAC Address, NetBIOS Name, NetBIOS Domain, Domain User, Domain Member, OS-Class, Switch Port, Switch Port VLAN, Switch Port Status, Switch Vendor hoặc tương đương.
Tính năng phân loại thiết bị theo cơ chế chủ động và bị động	- Giải pháp hỗ trợ các kỹ thuật: + Kỹ thuật phân tích chủ động (Query AD; MAC database; WMI; NMAP; SSH; SNMP; Agent-based inspection,…) hoặc tương đương. + Kỹ thuật phân tích bị động (SPAN; DHCP fingerprinting; TCP fingerprinting; HTTP user-agent,…) hoặc tương đương.
Tính năng tương thích với nhiều nhà cung cấp thiết bị mạng khác nhau	- Giải pháp phải tích hợp với hạ tầng mạng: có dây (wired), không dây (wireless) tương thích với các thiết bị chuyển mạch CIC đang sử dụng: Cisco CBS350-48T-4G, Cisco C9500-48Y4C, Cisco C1000/C1200/C1300. - Giải pháp có hỗ trợ 802.1x. - Giải pháp sau khi tích hợp cho phép thực hiện các hành động: gán VLAN cho port trên Switch, tắt port trên Switch, hỗ trợ đưa ra các chính sách truy cập động (Dymanic Access List). - Giải pháp cho phép triển khai trên hạ tầng mạng gồm nhiều thiết bị chuyển mạch của các hãng khác nhau mà không yêu cầu thiết bị hỗ trợ 802.1x.
Tính năng liên tục kiểm soát và tự động khắc phục trên các thiết bị đầu cuối không cần cài đặt Agent	- Giải pháp cho phép từ chối truy cập hoặc cách ly thiết bị trong quá trình tự khắc phục và khôi phục quyền truy cập sau khi hoàn tất việc khắc phục. - Giải pháp có khả năng tích hợp với công cụ quét lỗ hổng (Tenable, Qualys, Rapid7) hoặc tương đương.

Nội dung	Yêu cầu kỹ thuật
Tính năng kiểm tra tuân thủ của thiết bị đầu cuối không cần cài đặt Agent	- Giải pháp phải có khả năng định danh, đánh giá theo thời gian thực các thiết bị đầu cuối khi chúng kết nối vào mạng mà không cần khai báo trước về thiết bị đó. - Giải pháp phải có khả năng xác định thiết bị, phần mềm, dịch vụ, trạng thái bản vá và tình trạng của phần mềm antivirus để đảm bảo tuân thủ các chính sách bảo mật. - Giải pháp phải có khả năng tạo, chỉnh sửa hoặc thay đổi các chính sách tuân thủ từ đầu theo thiết kế và mục đích của tổ chức. - Giải pháp có khả năng phân loại và đưa ra chính sách với thiết bị laptop. - Giải pháp có khả năng phân loại và đưa ra chính sách với máy tính windows không đăng ký vào domain CIC. - Giải pháp có khả năng nhận diện người dùng sử dụng tài khoản cục bộ trên thiết bị đầu cuối.
Tính năng phân đoạn mạng	- Giải pháp phải có khả năng phân đoạn mạng động qua chính sách truy cập động (Dynamic Access List), gán vào mạng (VLAN) khác, chặn kết nối TCP hoặc tương tự. - Giải pháp phải có khả năng gán động vào mạng (VLAN) phù hợp với vai trò của người dùng hoặc thiết bị.
Tính năng phát hiện và phản ứng lại hành vi bất thường	- Giải pháp phải có khả năng theo dõi, phát hiện các hoạt động nghi ngờ như MAC Spoofing, ARP Spoofing trên các thiết bị đầu cuối.
Tính năng tích hợp với các hệ thống Quản lý Thông tin và Sự kiện An ninh (SIEM)	- Giải pháp phải có khả năng tích hợp với các hệ thống Quản lý Thông tin và Sự kiện An ninh (SIEM) của bên thứ 3 (Splunk, QRadar,…).
Tính năng quản trị và báo cáo	- Giải pháp cung cấp khả năng quản trị tập trung thông qua CLI / GUI. - Giải pháp phải có khả năng tạo các báo cáo theo các thông số khác nhau: Tuân thủ (Compliance), Không tuân thủ (Non-Compliance). - Giải pháp có khả năng tạo các báo cáo và trích xuất báo cáo theo định dạng: PDF, CSV. - Giải pháp phải có sẵn các định dạng báo cáo và cho phép tùy chỉnh theo yêu cầu.