

Số: /TB-STTTT

Tây Ninh, ngày tháng 6 năm 2022

THÔNG BÁO

Về việc chào giá “Nâng cấp khả năng xử lý của hệ thống giám sát, bảo mật đối với người dùng truy cập từ internet vào các hệ thống ứng dụng”

Căn cứ Quyết định số 848/QĐ-UBND ngày 07/4/2022 của Chủ tịch Ủy ban nhân dân tỉnh Tây Ninh Ban hành Kế hoạch chuyển đổi số và đảm bảo an toàn thông tin mạng tỉnh Tây Ninh năm 2022;

Sở Thông tin và Truyền thông Tây Ninh thông báo mời các đơn vị chào giá cung cấp dịch vụ “**Nâng cấp khả năng xử lý của hệ thống giám sát, bảo mật đối với người dùng truy cập từ internet vào các hệ thống ứng dụng**” chi tiết như phụ lục đính kèm.

Sở Thông tin và Truyền Thông kính mời quý đơn vị tham gia chào giá cạnh tranh cung cấp dịch vụ nêu trên.

Hồ sơ chào giá bao gồm Bảng chào giá cung cấp gói dịch vụ (Giá chào hàng bằng VNĐ, đã bao gồm thuế và chi phí triển khai, hỗ trợ cài đặt).

Thời gian nhận hồ sơ chào giá là 05 ngày tính từ ngày ra thông báo. Địa điểm nhận hồ sơ: 06 Trần Quốc Toản, Phường 2, Thành phố Tây Ninh, tỉnh Tây Ninh. Điện thoại: 0276 3 824666.

Trân trọng./.

Nơi nhận:

- Các Công ty cung cấp dịch vụ tin học;
- Lưu: VT, TTGSĐH.

GIÁM ĐỐC

PHỤ LỤC

Cung cấp dịch vụ: “Nâng cấp khả năng xử lý của hệ thống giám sát, bảo mật đối với người dùng truy cập từ internet vào các hệ thống ứng dụng”

- Địa điểm thực hiện: Trung tâm tích hợp dữ liệu tỉnh Tây Ninh

- Nội dung thực hiện:

STT	Sản phẩm	Mô tả	Số lượng	Đơn vị tính
1	Fortinet FortiWeb 1000E Web Application Firewall	<p>Hiệu suất và năng lực: Số cổng RJ45 built-in: 6 Số cổng RJ45 hỗ trợ bypass: 4 Số cổng SFP: 4 Số cổng SFP+: 2 Số cổng USB: 2 Dung lượng lưu trữ: 2000 GB GB Hỗ trợ nguồn: Dual Hot Swappable Throughput: 1.3 Gbps Gbps Độ trễ: 5 ms Số lượng miền quản trị: 64 Hỗ trợ cơ chế High Availability: Active/Passive, Active/Active, Clustering</p> <p>Tính năng: Chế độ triển khai: Reverse Proxy Inline Transparent True Transparent Proxy Offline Sniffing WCCP</p> <p>Thiết bị có tích hợp sẵn chip xử lý chuyên dụng để tăng tốc xử lý dữ liệu SSL/TLS Thiết bị tích hợp sẵn tính năng HTTPS/SSL Offloading Hỗ trợ bảo vệ API Interface sử dụng XML, JSON, RESTful, phân tích nội dung khi ứng dụng sử dụng và áp dụng xác thực chính sách bảo mật Hỗ trợ tính năng bảo vệ các trang web, ứng dụng dành cho thiết bị di động và API khỏi các</p>	01	Cái

		<p>mối đe dọa tự động bằng cách ngăn chặn truy cập bot dựa theo các thông tin nhận diện như: các sự kiện truy cập của người dùng, và các hành vi đáng ngờ.</p> <p>Anomaly detection</p> <p>Hỗ trợ cơ chế máy học 2 lớp bằng cách xây dựng các mẫu thử theo mô hình Hidden Markov Model (HMM) và giám sát quyền truy cập vào ứng dụng và thu thập dữ liệu để xây dựng mô hình toán học dựa trên truy cập HTTP để phát hiện, phân biệt hành vi truy cập bất thường, có nguy cơ tiềm ẩn hoặc bình thường, sau đó sẽ tự động thực hiện các tác vụ ngăn chặn</p> <p>Hỗ trợ chế độ kiểm tra tuân thủ an ninh thông tin ngăn chặn rò rỉ dữ liệu theo HIPAA, Sarbanes-Oxley Act (SOX), HITECH, PCIDSS</p> <p>Giải pháp có thể tích hợp với các sản phẩm tường lửa, phân tích mã độc cùng hãng tạo nên mạng lưới bảo mật mở rộng các biện pháp bảo vệ cơ bản thông qua đồng bộ hóa và chia sẻ thông tin về mối đe dọa để quét sâu các tệp đáng ngờ và chia sẻ các nguồn nội bộ bị nhiễm</p> <p>Giải pháp có khả năng tích hợp với các thiết bị dò tìm lỗ hổng bảo mật như Acunetix, HP WebInspect, IBM AppScan, Qualys, ImmuniWeb và WhiteHat để cung cấp các bản vá ảo cho các vấn đề bảo mật trong môi trường ứng dụng. Thiết bị tự động chuyển thành quy tắc bảo mật để bảo vệ ứng dụng cho đến khi các nhà phát triển có bản vá chính thức.</p> <p>Thiết bị đi kèm đầy đủ bản quyền sử dụng các tính năng AV, Security Service, và IP Reputation thời hạn 01 năm</p> <p>Hỗ trợ dịch vụ bảo hành phần cứng và hỗ trợ kỹ thuật 24/7 của hãng sản xuất, thời hạn 01 năm.</p>		
2	Modules SFP 10GE	10GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots	02	Cái
3	Modules SFP 1GE	1GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots	04	Cái