SPITALUL CLINIC JUDEȚEAN DE URGENȚĂ „PIUS BRÎNZEU" TIMIȘOARA

• Bulevardul Liviu Rebreanu, Nr. 156Timișoara, jud. Timiș, Cod Postal 300723
• Cod fiscal 4663448 • Telefon +4 0356 433111 • Fax +4 0256 486956
• e-mail: judetean@hosptm.ro • www.hosptm.ro

Sursa Surse Proprii Unitate Protejata
Nr. 17364 /29.03.2023

INVITAȚIE DE PARTICIPARE

1. Autoritate contractantă: **SPITAL CLINIC JUDEȚEAN DE URGENȚĂ "PIUS BRÎNZEU" TIMIȘOARA, Bv. Liviu Rebreanu, nr.156, Cod fiscal 4663448,Tel. 0356/433.127 Fax. 0356/433.114**

2. Tipul si durata contractului pentru care este solicitată ofertă: **Contract de Servicii , valabilitate pana la data de 31.12.2023.**

3. Procedura aplicată pentru atribuirea contractului de furnizare produse: **Achizitie directe**

4. Locul de executie : **SPITAL CLINIC JUDEȚEAN DE URGENȚĂ "PIUS BRÎNZEU" TIMIȘOARA**

Servicii de Securitate a Datelor cu Livrare de Echipament de tip Internal Firewall model Sophos XGS 3100

cod CPV 72500000-0

Valoarea estimata 44,820,00lei, exclusiv TVA. /An 3.735/Luna exclusiv TVA.

5. Oferta va conține:

Ofertanții,tertii susținatori și subcontractanții nu trebuie să se regăsească în situațiile prevăzute la art 164,165,167 din legea nr 98/2016.Modalitatea prin care poate fi demonstrate indeplinirea cerinței

.

Se va complecta o declarație pe propria raspundere de către operatorii economici participanți la procedura de atribuire cu informaiile aferente situației lor

Propunerea tehnică va respecta cerințele •Referat Necesitate nr 15370.15.03.2023 atașat

- **Documente atestare**
- **Propunerea financiară (va fi exprimată în lei, fără TVA, cu două zecimale) cu prezentare documente conform legea 448 (Unitate Protejata,)**
- **Autorizatia,fisa postului personalului angajat și certificatul medical de handicap acestor persoane cu handicap. pentru furnizar**
- **Propunerea financiară (va fi exprimată în lei, fără TVA, cu două zecimale si va fi pe pachet cu pretul pe fiacre produs)**

6. Durata de realizare a contractului:**31.12.2026.**

7. Se interzice depunerea de oferte alternative.

8. Termenul limită de primire a ofertelor:. **30.03.2023, ora 09^{00}**

• Bulevardul Liviu Rebreanu, Nr. 156 Timișoara, jud. Timiș, Cod Poștal 300723
• Cod fiscal 4663448 • Telefon +4 0356 433111 • Fax +4 0256 486956
• e-mail: judetean@hosptm.ro • www.hosptm.ro

Sursa Surse Proprii Unitate Protejata

9. Limba în care trebuie redactate oferetele: **română**

10. Data, ora, locul deschiderii ofertelor: **30.03.2023, ora 09[00] ofertele se depun pe adresa de E-mail florin.ambru@hosptm.ro , urmand ca oferta castigatoare va urcara oferta in catalogul electronic de achizitii publice SICAP.**

In cazul in care se constata doua sau mai multe oferte clasate pe primul loc cu acelasi pret, la solicitarea comisiei de evaluare se va depune o noua oferta online la o data stabilita de catre comisie. Preturile noi ofertate nu pot depasi valoarea ofertata anterior.

Pentru ofertantii care nu vor prezenta o noua oferta de pret respectiv, nu vor transmite oferta finala pana la datele stabilite de catre comisia de evaluare se va lua in considerare valoarea din oferta anterioara, respectiv oferta initiala. Procesul de reofertare se va desfasura intr-o singura etapa.

11. Modalităţi principale de finanţare şi de plată şi/sau referirile la prevederile care le reglementează: **Sursa de Finantare Surse Proprii Unitate Protejata**

12. Termenul de plată al facturilor este de 30 de zile de la data primirii facturii de către Achizitor.

13. Perioada pentru care ofertantul trebuie să îşi menţină oferta valabilă: **90 de zile de la data de deschidere a ofertelor.**

14. Alăturat vă transmitem:

Referat Necesitate nr 15370.15.03.2023

Prof.Univ.Dr Dorel Săndesc

Manager

[redacted]

Şe i Pubice,

In

[redacted]

Şef B

Vasile

[redacted]

Întocmit Referent,
Ec Florin Ambru

[redacted]

SPITALUL CLINIC JUDEȚEAN DE URGENȚĂ „PIUS BRÎNZEU" TIMIȘOARA

• Bulevardul Liviu Rebreanu, Nr. 156Timișoara, jud. Timis, Cod Postal 300723
• Cod fiscal 2563448 • Telefon +4 0356 433111 • Fax +4 0256 486936
• e-mail: judeteana@hosptm.ro • www.hosptm.ro

ANMCS
unitate aflată în PROCES DE ACREDITARE
CICLUL al III-lea

SPITALUL CLINIC JUDEȚEAN DE URGENȚĂ „PIUS BRÎNZEU" TIMIȘOARA
INTRARE IEȘIRE
NR. 15370

Aprobat
Manager
Prof.dr. Dorel Săndesc

Avizat
Director financiar contabil
Ec. Pogacean Ali

MAR 2023

REFERAT DE NECESITATE
Nr. ..... / 15.03.2023

Categorie necesitate: **Lucrari** ☐ **Servicii** ■ **Produse** ☐ **Urgență** ☐
Tip necesitate: **Anual** ☐ **Lunar** ■ **Ocazional** ☐

Subsemnatul ing. Lucian Bosneag în calitate de Responsabil NIS în cadrul Spitalului Clinic Județean de Urgență Timișoara,

Vă rugăm să aprobați achiziționarea următoarelor produse/servicii: "Servicii de securitate a datelor cu livrare de echipament de tip internal firewall model Sophos XGS 3100 cu menținerea la zi a certificatelor și mentenanța hardware. Licentiere de certificate este pentru 3 ani".

Necesar, având în vedere motivele detaliate în cele ce urmează:

Descriere necesitate (inclusiv motivarea): Echipamentul integrat de tip „Next-Generation Firewall intern" dispune atât de capabilități avansate de securitate, de prevenire a intruziunilor, control al aplicațiilor, VPN, cât și de capabilități de rutare a traficului de date, destinat folosirii ca o soluție de securitate unificată, necesar pentru asigurarea securității și confidențialității datelor din rețeaua SCJUPBT. Acest echipament este o soluție necesară conform legii securității cibernetice.

Pentru acest echipament este necesar a se respecta toate specificațiile tehnice cerute, având în vedere obligația satisfacerii tuturor cerințelor de compatibilitate (cu predilecție pentru asigurarea securității cibernetice) cu echipamentele deja existente în dotarea SCJUPBT.

Valoarea estimată a contractului este de 3735 lei / lună / 3 ani.

Specificațiile tehnice sunt anexate prezentului referat.
Cantitatea din STOC sectiei la data emiterii referatului: - (U.M. – buc, etc)
Valoare estimată de către inițiator: ..... lei
Sursă de finanțare (Buget CAS, Buget program national –denumire): PROPRII

Întocmit: Ing. Lucian Bosneag – Responsabil NIS

Confirm necesitatea (șef secție/compartiment/serviciu/birou) Dr.ing. Mariana Moga

Repartizat catre:
Data: 16-03-2023
Valoare estimata confirmata:
Exista acord-cadru/contract: DA ☐ NU ☒
Procedura aflata in desfasurare: DA ☐ NU ☒
Necesita caiet de sarcini: DA ☐ NU ☐
Nota: (in cazul se va bifa DA, se va redirectiona către omitentul caietului de sar
Semnatura:

Serviciul Achizitii Publice – Contractare
Tip procedura _____
Semnatura:

27-03-2023

SPECIFICAȚII TEHNICE

"Servicii de securitate a datelor cu livrare de echipament de tip internal firewall model Sophos XGS 3100 cu menținerea la zi a certificatelor și mentenanța hardware. Licentierea de certificate este pentru 3 ani".

Descriere generală

Echipamentul integrat de tip „Next-Generation Firewall intern" dispune atât de capabilități avansate de securitate, de prevenire a intruziunilor, control al aplicațiilor, VPN, cât și de capabilități de rutare a traficului de date, destinat folosirii ca o soluție de securitate unificată, necesar pentru asigurarea securității şi confidenţialităţii datelor din reţeaua SCJUPBT. Acest echipament este o soluție necesară conform legii securității cibernetice.

Specificații hardware

CPU (Core/Threads): 4
CPU (Memory): 12GB
NPU (Core/Threads): 20
NPU (Memory): 4 GB
Spatiu local de stocare SSD, min.: 240 GB
Interfete ethernet RJ45: 8 x GE copper, 2 x SFP fiber, 2 x SFP+ 10 GbE fiber
Porturi administrare: 1 x RJ45 MGMT, 1 x COM (RJ45), 1 x Micro-USB
Alte porturi: 2 x USB 3.0, 1 x USB 2.0
Module (optional): 8-porturi GbE RJ45, 8-porturi GbE SFP fiber, 4-porturi 10 GE SFP+ fiber, 4-porturi GbE RJ45 (2 perechi), 4-porturi GbE RJ45 PoE +, 4-porturi GbE RJ45, 4-porturi 2.5 GbE RJ45 PoE
Max. POE (cu modul optional): 1 modul cu 4 ports, max. 60 W
Display: Display multifunctional LCD

Performanța sistemului

Firewall throughput: 47,000 (Mbps)
Firewall IMIX: 23,000 (Mbps)
Firewall Latency (64 byt UDP): 4 µs
IPS throughput: 10,000 (Mbps)
NGFW: 9,000 (Mbps)
Threat Protection throughput: 2,000 (Mbps)
SSL/TLS: 2,400 (Mbps)
Conexiuni concurente: 12,000,000
Conexiuni noi/sec: 185,000
IPsec VPN: 25,000 (Mbps)
IPsec VPN concurrent tunnels: 6,500
SSL VPN concurrent tunnels: 5,000

Alimentare si dimensiuni
Surse alimentare curent alternativ
Sursă alimentare redundantă, optionala
Montabil în rack, spatiul ocupat de echipament maximum 1RU
Max. POE si/sau cu modul optional: max. 60 W
Consum: min 55 W (in standby), max 190 W (echipat complet)

Suport High Availability
Activ/Activ
Activ/Pasiv cu Stateful Failover
Link monitoring

Servicii securitate
Echipamentul trebuie să acționeze în conformitate cu principiul „Minimal Privilege", adică să blocheze toate aplicațiile, indiferent de portul TCP/IP, cu excepția celor permise explicit și pentru care sunt indicate normele de politica de securitate.
Echipamentul trebuie să permită crearea manuală de semnături pentru aplicații adiționale, direct pe dispozitiv în interfața de administrare, fără a necesita instrumente externe sau implicarea producătorului.
Echipamentul trebuie sa permita detectia de noi semnaturi, crearea de filtre in functie de semnaturile noi adaugate si optional posibilitatea de a obtine noi semnaturi de la agentul instalat pe statiile de lucru. Echipamentul trebuie sa permita definirea de actiuni de tip blocare sau continuare pentru prevenirea atacurilor de tip "Zero-day" prin afișarea unei pagini care informează utilizatorul și eventual permite continuarea download-ului dupa acceptul utilizatorului.
Echipamentul trebuie să asigure inspecția traficului criptat SSL/TLS inclusiv pentru comunicații ce nu folosesc protocol HTTP, și sa realizeze inspecția traficului decriptat pentru detecție Antivirus, Antispyware, IPS si pentru blocare de fisiere.
Echipamentul trebuie sa suporte scanarea cu multiple motoare de cautare antivirus (minim 2).
Echipamentul trebuie să poată fi configurat cu un set de politici de decriptare și inspecție specifică a traficului SSL/TLS separat de politicile de securitate a traficului decriptat.
Echipamentul trebuie să permită configurarea profilelor de identificare IPS în mod specific pentru fiecare regulă de securitate în parte. Nu se acceptă ca scanarea IPS să se realizeze doar la nivelul întregului echipament sau doar pentru interfețe specifice.
Echipamentul trebuie sa permita blocarea adreselor WEB atat pe categorii predefinite cat si individual, posibilitatea creeri de exceptii globale cat si individuale per user sau/si workstation.
Echipamentul trebuie sa permita optiunea de securitate sincronizata, izolare automata a dispozitivului compromis, pana la rezolvarea incidentului, verificarea automata a retelei pe baza semnaturii detectate pe sistemul compromis.

Functionalitati firewall

Suport NAT (SNAT, DNAT, PAT, Static NAT)

Configurarea regulilor NAT poate sa fie independenta de configurarea protocoalelor, mecanismelor de rutare sau in legatura directa cu o regula firewall.

Rutare dinamica - RIP, OSPF, OSPFv3, BGP, Multicast, SD-WAN

Functionalitati SD-WAN cu posibilitatea de ruta trafic in functie de aplicatie, serviciu sau user

Sistemul de operare al echipamentului trebuie sa permita crearea de reguli/profile de redistribuire a rutelor dintr-un protocol de rutare dinamica in altul.

VLAN Tagging (802.1q)

Profilele de inspectie a traficului de retea si implicit, a continutului, trebuie poata fi aplicate granular pentru fiecare regula de firewall.

Profilele de control al aplicatiilor si gestionarea filtrarii WEB, trebuie sa poata fi aplicate granular pentru fiecare regula de firewall.

Functionalitati VPN

IPsec Site-to-Site

IPSec, SSL Remote Access

Algoritmi de criptare suportati pentru IPsec faza 1: AES 128, AES 192, AES 256, 3DES

Algoritmi de hashing suportati pentru IPsec faza 1: SHA-1/SHA-256/SHA-384/ SHA-512

Algoritmi de criptare suportati pentru IPsec faza 2: AES 128, AES 192, AES 256, 3DES, AES 128GCM, AES 192GCM, AES 256GCM, AES 128GMAC, AES 192GMAC, AES 256GMAC

Algoritmi de hashing suportati pentru IPsec faza 2: SHA-1/SHA-256/SHA-384/ SHA-512

Grupuri DH suportate pentru IPsec faza 1: DH5, DH14, DH19, DH21, DH26, DH31

Grupuri DH suportate pentru IPsec PFS: DH5, DH14, DH21, DH26, DH31

Suport VPN tip client de tip IPsec si SSL VPN

Autentificare IKEv1 si IKEv2 cu PSK sau Certificate

Suport IPSec NAT Traversal

Functionalitati pentru prevenirea intruziunilor

Suport indentificare anomalii ale protocoalelor

Suport semnături definite de utilizator

Suport IPv6:

Filtrare aplicatii in functie de categorie

Activitati curente: useri si conexiuni

Metode de diagnosticare: ping, traceroute, name lookup, route lookup, packet capture

DNS: lookup, reverse name lookup

DHCP: server, client, relay, dynamic lease scope, static lease scope, DNS/WINS server
Hosts and services: IP, IP groups, ICMP
IPS: DoS bypass rule, policies, spoof protection
IPv6 tunneling: 6in4, 6to4, 6rd, 4in6
Network address translation (NAT)
Neighbor Discovery Protocol (NDP)
Management over IPv6 (consola web pentru administrare)
VPN: IP-sec, SSL
Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
Interfata conexiuni prestabilite: LAN, WAN, DMZ, LOCAL, VPN, and Wi-Fi
Static routing: unicast route
Syslog
Policy-based routing
Reporting
Upstream proxy
VPN: IPsec site-to-site, remote access
Filtrare WEB in functie de categorie
Rutare: static, multicast (PIM-SM), si dinamic (RIP, BGP, OSPF) cu suport 802.1Q VLAN
Analiza statica si dinamica a fisierelor
Protectie Email si managementul carantinei emailului (optional)

Capabilitate de inspectie in sniffing mode (bridge sau tap)

Functionalitati inspectie continut

Suport Antispyware
Suport pentru sandboxing doar prin adaugarea ulterior a unei subscriptii
Suport pentru blocarea fișierelor în funcție de tip, pe baza header-ului fisierului
Suport pentru crearea de reguli distincte de blocare a fisierelor per aplicatie, indiferent de port TCP/IP, diferentiat upload/download, definite in cadrul regulilor de securitate firewall

Functionalitati filtrare URL-uri

Firewall-ul comunica constant cu cloud-ul aceluiasi producator pentru actualizarea listei cu URL-urile categorisite care nu fac parte deja din baza de date locala sau din cache-ul local al firewall-ului.
URL-urile pot fi plasate in mai multe categorii, oferind posibilitatea de a descrie granular continutul, scopul si gradul de risc ale site-ului accesat.
Echipamentul trebuie să asigure, fără componente hardware sau software adiționale, filtrarea accesului Web în funcție de categorii de conținut
Baza de date cu URL-uri și categoriile de conținut trebuie să fie actualizată regulat în mod automat (pe baza de subscripție la serviciul de actualizare al producătorului echipamentului)

Management
Administrare prin consola, SSH, HTTPS, CLI
Permite configurarea tuturor functionalitatilor fara software aditional de management
Permite crearea de utilizatori/administratori cu drepturi configurabile pe baza rolurilor acestora
Syslog, SNMP, log-uri interne, grafice, notificări e-mail, consola centralizata.
Capabilitate de export de loguri filtrate pe baza regulilor definite de administrator.
Capabilitate de export diferentiat pentru fiecare regula de securitate in parte
Capabilitate de management complet prin API de tip web/xml
Backup: configurația trebuie să se poată salva și restaura sub forma unui fișier text/xml. Posibilitatea de transmitere criptata automata a fisierului de backup prin FTP sau email.

Functionalitati autentificare
Baza de date locala
Integrare Active Directory
Integrare LDAP/Radius/TACACS+, eDirectory server
Integrare administrare SSO Azure AD
Integrare directa cu Microsoft AD, Exchange, RADIUS, Syslog, Web API pentru identificarea utilizatorilor din LDAP/AD cu adresa IP.
Capabilitate de a forta autentificare multifactor pentru accesul catre o zona sau un grup de servere.

Licentiere
Fara limitare a numarului de adrese IP prin licentiere
Fara limitare a numarului de utilizatori IPsec VPN/SSL VPN
Fara limitare pentru suport IPv6 prin licentiere
Licențe pentru activarea actualizărilor serviciilor IPS, filtrare WEB, control aplicatii, protectie malware, protectie antivirus, Zero-day/Sandstorm pe o perioada de minim 3 ani.
Asigurarea suportului din partea producatorului pentru o perioada de minim 3 ani.
Interfețele să fie active la viteza maximă

Service și garanție
Garanție: 3 ani
Update software gratuit: 3 ani
Update semnături: 3 ani

Alte cerințe:

- servicii de suport tehnic 24/7, 365 zile pe an, oferit de producător;

- mentenanță on-site, cu termen de intervenție de 1 oră de la sesizare;

Pentru acest echipament este necesar a se respecta toate specificaţiile cerute, având în vedere obligaţia satisfacerii tuturor cerinţelor de compatibilitate (cu predilecţie pentru asigurarea securităţii cibernetice) cu echipamentele deja existente în dotarea SCJUPBT.

Dr.ing. Mariana Moga

Șef Serviciu Informatic