„Pro-Medica" w Ełku Sp. z o.o.
19-300 Ełk, ul. Baranki 24,
tel. 87 620-95-71 wew. 51 - Automatyczna Centrala
tel. 87 621-96-20 - Sekretariat, Zarząd Spółki

Dział Zaopatrzenia i Zamówień Publicznych
tel. 87 620-95-93
tel. 87 620-95-76
tel. 87 620-96-26

e-mail: zaopatrzenie-pm@elk.com.pl
e-mail: przetargi@promedica.elk.pl
www.promedica.elk.com.pl

Odpowiedź na Zapytanie 8

Wszyscy uczestnicy postępowania

Znak: P-M/Z/ 5713 /2021 **Data: 03.12.2021r.**

Dotyczy: przetargu nieograniczonego na **Zakup urządzeń sieciowych, pozostałej infrastruktury sprzętowej i oprogramowania wraz z wymaganymi integracjami** w ramach realizacji projektu „Wdrożenie elektronicznej dokumentacji medycznej oraz uruchomienie e-usług w "Pro-Medica" w Ełku Sp. z o. o." RPWM.03.02.00-28-0018/20-00 projekt realizowany ze środków Europejskiego Funduszu Rozwoju Regionalnego Regionalnego Programu Operacyjnego Województwa Warmińsko-Mazurskiego na lata 2014-2020." Działanie 3.2 E-zdrowie. **Znak sprawy: 4563/2021.**

Na podstawie art. 135 ust. 1-2 ustawy Prawo zamówień publicznych (t.j. Dz. U. z 2021 r. poz. 1129) Zamawiający przekazuje treść zapytań dotyczących zapisów specyfikacji warunków zamówienia wraz z wyjaśnieniami. W przedmiotowym postępowaniu wpłynęły następujące pytania:

PYTANIE nr 1
Dotyczy PAKIETU 3 – Zakup i instalacja infrastruktury sprzętowej (urządzenia sieciowe)
Po konsultacji z przedstawicielami dystrybutorów bezpieczeństwa IT w Polsce informujemy, że opis wymagań minimalnych przedmiotu zamówienia dla pakietu 3, nie daje możliwości zaoferowania jednego z najbardziej popularnych i najsilniejszych producentów europejskich który w ostatnim czasie został nagrodzony certyfikatem „Cybersecurity made in Europe" wydawanym przez ESCO, a zgodny z kryteriami ENISA. W związku z powyższym wnioskujemy do Zamawiającego o dopuszczenie kluczowego, europejskiego producenta rozwiązań Next Generation Firewall do postępowania poprzez dopuszczenie parametrów równoważności wskazanych poniżej. Dodatkowo Informujemy Zamawiającego, że dzięki dopuszczeniu europejskiego rozwiązania, Zamawiający podnosi również poziom bezpieczeństwa swojej organizacji dając szansę na zaoferowanie technologii europejskiej w tak trudnych czasach, gdzie zaufanie do technologii jest kluczowe. Dodatkowo gwarantujemy Zamawiającemu, że obniży to koszty utrzymania i licencji rozwiązania w przyszłości. Rozwiązanie posiada certyfikaty takie jak: NATO Restricted, EU Restricted, EAL3+ oraz EAL4+. **W związku z powyższym czy Zamawiający dopuści możliwość zaoferowania rozwiązań o poniższych parametrach jako równoważne do wskazanych w dokumentacji przetargowej**
1/ System bezpieczeństwa Next Generation Firewall:

Wymagania wspólne:
Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. Dla elementów systemu bezpieczeństwa wykonawca musi zapewnić wszystkie poniższe funkcjonalności:

UTM TYP 1- 1 sztuka

- Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
- System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000
- System realizujący funkcję Firewall musi umożliwiać rozszerzenie dostępnych interfejsów o minimum 2 interfejsy optyczne 10GbE (SFP+)
- Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
- W zakresie Firewall'a obsługa nie mniej niż 1 500 000 jednoczesnych połączeń oraz 75 000 nowych połączeń na sekundę.
- System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 120 GB do celów logowania i raportowania.
- Wydajność systemu Firewall minimum 20 Gbps
- Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus minimum 2 Gbps
- Wydajność ochrony przed atakami (IPS) minimum 11 Gbps
- Wydajność VPN IPSec, nie mniej niż 4 Gbps

UTM TYP 2 – 1 sztuka

- Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
- System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000.
- Możliwość tworzenia minimum 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
- W zakresie Firewall'a obsługa nie mniej niż 300 tys. jednoczesnych połączeń oraz 15 tys. nowych połączeń na sekundę.
- System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
- System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 64 GB lub pozwalać na zbieranie logów na zewnętrznym dysku, pendrive lub karcie SD o pojemności co najmniej 64 GB do celów logowania i raportowania
- Wydajność systemu Firewall minimum 3,5 Gbps
- Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus minimum 450 Mbps
- Wydajność ochrony przed atakami (IPS) minimum 1,6 Gbps
- Wydajność VPN IPSec, nie mniej niż 500 Mbps

UTM TYP 3 – 1 sztuka

- Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
- System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000.
- Możliwość tworzenia minimum 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
- W zakresie Firewall'a obsługa nie mniej niż 150 tys. jednoczesnych połączeń oraz 15 tys. nowych połączeń na sekundę.

🕐 System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
🕐 System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 16GB lub pozwalać na zbieranie logów na zewnętrznym dysku, pendrive lub karcie SD o pojemności co najmniej 16GB do celów logowania i raportowania.
🕐 Wydajność systemu Firewall minimum 2 Gbps
🕐 Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus minimum 350 Mbps
🕐 Wydajność ochrony przed atakami (IPS) minimum 1.6 Gbps
🕐 Wydajność VPN IPSec, nie mniej niż 300 Mbps

Wymagania wspólne:
🕐 W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:
✓ Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
✓ Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS); System AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.
✓ Poufność danych - IPSec VPN oraz SSL VPN
✓ Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
✓ Kontrola stron Internetowych – Web Filter [WF]
✓ Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3
✓ Kontrola pasma oraz ruchu [QoS i Traffic shaping]
✓ Kontrola aplikacji oraz rozpoznawanie ruchu P2P
✓ Analiza ruchu szyfrowanego protokołem SSL
🕐 System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
🕐 W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
✓ Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site
✓ Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem
✓ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
✓ Praca w topologii Hub and Spoke oraz Mesh
✓ Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth
🕐 Obsługa ssl vpn w trybach portal oraz tunel
🕐 Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
🕐 Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
🕐 Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
🕐 Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
🕐 Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
🕐 Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
🕐 Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
🕐 Baza filtra WWW pogrupowana w min 50 kategorii tematycznych.
🕐 Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
🕐 Automatyczne ściąganie sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.

🕐 System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
✓ Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
✓ Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
✓ Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych
✓ Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny
🕐 W zakresie realizowanych funkcjonalności systemu raportowania i przeglądania logów, wymagane jest nie mniej niż:
✓ Posiadanie predefiniowanych raportów dla ruchu WWW, modułu IPS, skanera antywirusowego i antyspamowego
✓ Generowanie co najmniej 25 różnych typów raportów
🕐 System raportowania i przeglądania logów wbudowany w system bezpieczeństwa nie może wymagać dodatkowej licencji do swojego działania
🕐 System firewall musi:
✓ posiadać certyfikat Common Criteria EAL4+
✓ posiadać certyfikat ICSA Labs dla funkcji: VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE
🕐 Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
🕐 Wymaga się, aby dostawa obejmowała również:
✓ Minimum 60-miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu.
✓ Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 60 miesięcy liczoną od dnia zakończenia wdrożenia całego systemu.

Odpowiedź: Zamawiający nie dopuści.

Wykonawcy zobowiązani są do uwzględnienia w ofercie treści udzielonych odpowiedzi i dokonanych zmian, stanowią one bowiem integralną część SWZ.

Z poważaniem