2025-195691

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest **aktualizacja systemu bezpieczeństwa poprzez dostawę urządzeń typu firewall dla Centrum e-Zdrowia w Warszawie.**

1. **Termin realizacji zamówienia:** do 60 dni kalendarzowych.

2. **Zamówienie obejmuje:**

2.1. Dostawę urządzeń i oprogramowania opisanych szczegółowo w pkt. 4, 5,

2.2. Świadczenie usługi gwarancji na dostarczone urządzenia i system opisane w pkt. 6,

3. **Opis systemu:**

Zamawiający posiada:

3.1. System zabezpieczeń – urządzenia FortiGate-20C, FortiGate-60D

3.2. System do analizy zdarzeń oraz logów – FortiAnalyzer

3.4 System zarządzający – FortiManager

4. **Urządzenia typu Firewall - 25 sztuk.**

L.p.	Cecha	Wymagania minimalne i jakościowe
4.1.	Wymagania ogólne	Dostarczony system bezpieczeństwa musi być kompatybilny i zapewnić współpracę z posiadanymi przez Zamawiającego urządzeniami i systemami (pkt.3) oraz zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia. Oferowane Urządzenie w dniu składania ofert nie może być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
4.2.	Tryby pracy	System realizujący funkcję Firewall musi dawać możliwość pracy w trybie routera z funkcją NAT.
4.3.	Zasilanie	System musi być wyposażony w zasilanie AC.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

L.p.	Cecha	Wymagania minimalne i jakościowe
4.4.	Wydajność	• W zakresie Firewall'a obsługa nie mniej niż 500 000 jednoczesnych sesji oraz 30 000 nowych połączeń na sekundę. • Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 3.5 Gbps.
4.5.	Polityki	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
4.6.	Translacja	System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu.
4.7.	IPSec VPN	System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Tworzenie połączeń typu Site-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
4.8.	Routing	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu.
4.9.	WAN	System musi umożliwiać obsługę łącza WAN.
4.10.	Zarządzanie	Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
4.11.	Logowanie	System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

L.p.	Cecha	Wymagania minimalne i jakościowe
		W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Musi istnieć możliwość logowania do serwera SYSLOG.
4.12.	Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus, Web Filtering na okres 36 miesięcy.
4.13.	Wyposażenie	Urządzenie powinno być wyposażone w: • 1 port WAN • Minimum 2 porty 1GE RJ45
4.14.	Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta oraz Wykonawcy przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

5. <u>Urządzenia typu Firewall – 4 sztuki.</u>

L.p.	Cecha	Wymagania minimalne i jakościowe
5.1.	Wymagania ogólne	Dostarczony system bezpieczeństwa musi być kompatybilny i zapewnić współpracę z posiadanymi przez Zamawiającego urządzeniami i systemami (pkt.3) oraz zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia. Oferowane Urządzenie w dniu składania ofert nie może być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
5.2.	Tryby pracy	System realizujący funkcję Firewall musi dawać możliwość pracy w trybie routera z funkcją NAT.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

L.p.	Cecha	Wymagania minimalne i jakościowe
5.3.	Zasilanie	System musi być wyposażony w zasilanie AC.
5.4.	Wydajność	• W zakresie Firewall'a obsługa nie mniej niż 700 000 jednoczesnych sesji oraz 35 000 nowych połączeń na sekundę. • • Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 6.5 Gbps.
5.5.	Polityki	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5.6.	Translacja	System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu.
5.7.	IPSec VPN	System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Tworzenie połączeń typu Site-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
5.8.	Routing	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu.
5.9.	WAN	System musi umożliwiać obsługę łącza WAN.
5.10.	Zarządzanie	Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
5.11.	Logowanie	System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

L.p.	Cecha	Wymagania minimalne i jakościowe
		postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Musi istnieć możliwość logowania do serwera SYSLOG.
5.12.	Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus, Web Filtering na okres 36 miesięcy.
5.13.	Wyposażenie	Urządzenie powinno być wyposażone w: • Minimum 1 port WAN • Minimum 1 port DMZ • Minimum 4 porty 1GE RJ45
5.14.	Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta oraz Wykonawcy przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

6. Usługi gwarancji i gwarancja jakości

Lp.	Cecha	Wymagania minimalne
6.1.	Usługi gwarancji i gwarancja jakości	Wymagana jest 36 miesięczna gwarancja jakości oraz 36 miesięczna usługa gwarancji na dostarczone urządzenia i system. W obrębie gwarancji zawarte musi być: • W ramach usług gwarancji - dostęp do aktualnych wersji oprogramowania oraz dokumentacji producenta oraz wsparcie producenta lub Wykonawcy, • Sposób obsługi zgłoszeń gwarancyjnych w trybie 7x24, • W ramach gwarancji jakości - naprawa nastąpi w ciągu 24 godzin od zgłoszenia awarii. Jeżeli zasadna będzie wymiana sprzętu, nastąpi to najdłużej w ciągu 2 Dni roboczych od zgłoszenia awarii. W przypadku zasadności wymiany sprzętu, nośniki danych zostają u Zamawiającego.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

7. Aspekty środowiskowe

Wykonawca zobowiązany jest przedstawić oświadczenie potwierdzające zgodność dostarczonych Urządzeń w szczególności:

Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Zaoferowane urządzenia powinny być energooszczędne.

Dopuszcza się przedstawienie certyfikatu TCO, EPEAT lub normy ISO 14001

Nazwy własne oraz sformułowania określone przez Zamawiającego zostały użyte ze względu na posiadane przez niego rozwiązania technologiczne.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706