2024-112727

OPIS PRZEDMIOTU ZAMÓWIENIA

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

1. **Termin realizacji zamówienia:** do 50 dni od dnia podpisania umowy.
2. **Zamówienie obejmuje:**

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

2.2. Wdrożenie opisane w pkt 5,

2.3. Świadczenie usług gwarancji na dostarczone urządzenia i system opisane w pkt 6,

2.4. Dostawa zostanie zrealizowana do dwóch ośrodków przetwarzania danych Zamawiającego zlokalizowanych na terenie Warszawy.

3. **Opis systemu:**

Zamawiający posiada system zabezpieczeń - urządzenia FortiGate-6301F oraz FortiGate-601E.

4. **Urządzenia typu Firewall (4 sztuki):**

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 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.
4.2.	Tryby pracy	System realizujący funkcję Firewall musi dawać możliwość pracy w każdym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
4.3.	Instancje systemu	W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 10 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.
4.4.	Wsparcie dla IPv4 oraz IPv6	System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall; • Ochrony w warstwie aplikacji; • Protokołów routingu dynamicznego.

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
4.5.	Redundancja	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive w ramach dostarczanych urządzeń. W obu trybach musi istnieć funkcja synchronizacji sesji firewall. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
4.6.	Monitoring	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN.
4.7.	Interfejsy	System realizujący funkcję Firewall musi dysponować minimum: • 2 portami Gigabit Ethernet RJ-45; • 32 portami SFP28 25Gbps; • 6 gniazdami QSFP 40Gbps; • W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4.8.	Dysk	• System realizujący funkcję Firewall musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 2 TB.
4.9.	Zasilanie	System musi być wyposażony w redundantne zasilanie AC.
4.10.	Wydajność	• W zakresie Firewall'a obsługa nie mniej niż 120 mln jednoczesnych sesji oraz 1 mln nowych połączeń na sekundę. • Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji (HTTP 64K): nie mniej niż 135 Gbps. • Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 165 Gbps. • Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control- minimum 65 Gbps.
4.11.	Bezpieczeństwo	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje: • Kontrola dostępu - zapora ogniowa klasy Stateful Inspection; • Kontrola Aplikacji; • Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN; • Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS; • Ochrona przed atakami - Intrusion Prevention System; • Kontrola stron WWW; • Zarządzanie pasmem (QoS, Traffic shaping).

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
		• Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP); • Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site; • Analiza ruchu szyfrowanego protokołem SSL; • Analiza ruchu szyfrowanego protokołem SSH.
4.12.	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.
4.13.	Translacja	System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu; • Dedykowany ALG (Application Layer Gateway) dla protokołu SIP.
4.14.	Strefy bezpieczeństwa	W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4.15.	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 w trybie pracy Galois/Counter Mode(GCM); • Obsługa protokołu Diffie-Hellman grup 19 i 20; • Wsparcie dla pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE; • Tworzenie połączeń typu Site-to-Site oraz Client-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; • Mechanizm „Split tunneling” dla połączeń Client-to-Site.
4.16.	SSL VPN	System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym

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
		zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.; • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
4.17.	Routing	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego; • Policy Based Routingu; • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
4.18.	WAN	System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
4.19.	Zarządzanie pasmem	System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
4.20.	Kontrola antywirusowa	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
4.21.	Ochrona przed atakami	Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, długości parametrów URL, Cookies. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
4.22.	Kontrola aplikacji	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

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
		Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
4.23.	Kontrola WWW	Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance. Filtr WWW musi dostarczać kategorii stron zabronionych prawem np.: hazard, pornografia małoletnich. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
4.24.	Uwierzytelnianie	System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu; • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP; • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4.25.	Zarządzanie	Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny

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
		mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
4.26.	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. 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.
4.27.	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.
4.28.	Wyposażenie	Urządzenie powinno być wyposażone w: • 4 wkładek 100GE QSFP28 SR; • 2 wkładek 40GE QSFP+ SR; • 32 wkładki 25GE SFP28 SR; • okablowanie niezbędne do podłączenia urządzeń zewnętrznych;

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
		• wszelkie niezbędne komponenty potrzebne do zamontowania dostarczonych urządzeń w szafach RACK (np. organizery) oraz podłączenia do sieci energetycznej
4.29.	Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta lub 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. Wdrożenie

Wykonawca opracuje projekt wdrożeniowy oraz dokumentację powykonawczą dla oferowanego systemu i rozbudowy urządzeń zawierające co najmniej:

5.1. Dla projektu wdrożeniowego:

5.1.1. diagramy połączeniowe dla wszystkich komponentów sieci zamawiającego powiązanych z dostarczonymi urządzeniami,

5.1.2. konfigurację przewidzianą dla wszystkich urządzeń oraz propozycje zmian dla istniejących urządzeń połączonych z przedmiotem zamówienia,

5.1.3. harmonogram wdrożenia,

5.1.4. koncepcję testów następujących po wszystkich etapach wdrożenia,

5.1.5. plan awaryjny „backout" dla każdego kroku wdrożenia,

5.1.6. koncepcję testów redundancji wykonywanych po zakończeniu wdrożenia.

5.2. Dla dokumentacji powykonawczej:

5.2.1. diagramy połączeń,

5.2.2. opis wszystkich funkcjonalności wdrożonych podczas uruchamiania systemu,

5.2.3. pełne konfiguracje urządzeń,

5.2.4. wyniki testów redundancji.

5.3. W ramach wdrożenia Wykonawca zobowiązany jest do:

5.3.1. instalacji fizycznej urządzeń,

5.3.2. podłączenia kabli,

5.3.3. konfiguracji urządzeń niezbędnej do uruchomienia (adresacja interfejsów, konfiguracja uwierzytelniania, konfiguracja usług NTP, DNS, SNMP, Syslog),

5.3.4. instalacji i konfiguracji systemu do zarządzania urządzeniami,

5.3.5. konfiguracja odpowiednich systemów wirtualnych,

5.3.6. konfiguracji klastrów HA.

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

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.

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