Fundusze Europejskie na Rozwój Cyfrowy

Nasz znak: IZP.272.I.6.2024

ZAPYTANIE OFERTOWE

o udzielenie zamówienia publicznego z wyłączeniem stosowania ustawy Prawo zamówień publicznych, dotyczące udzielenia zamówienia publicznego o wartości od 50 000,01 zł netto do 129 999,99 zł netto

Dostawa UTM, UPS i serwerów do kopii zapasowych wraz z dyskami

WICESTAROSTA CHOSZCZEŃSKI
/-/ Stanisław Rydz

STAROSTA CHOSZCZEŃSKI
/-/ Wioletta Kaszak

Choszczno, 18 listopada 2024 r.

Fundusze Europejskie na Rozwój Cyfrowy

1. Nazwa i dane adresowe Zamawiającego

Zamawiający:	Powiat Choszczeński
Adres:	ul. Nadbrzeżna 2, 73-200 Choszczno
Telefon:	+ 48 95 748-89-30
E-mail:	sekretariat@powiatchoszczenski.pl
ESP (ePUAP)	/spowchoszczno/skrytka
Strona internetowa:	http://www.powiatchoszczenski.pl
Strona BIP:	https://bip.powiatchoszczenski.pl
NIP:	594-16-04-431
REGON:	210467244
Godziny urzędowania:	poniedziałek 7:30 – 15:30 wtorek 7:30 – 15:30 środa 7:30 – 15:30 czwartek 7:30 – 15:30 piątek 7:30 – 15:30

2. Wstęp

Zamówienie jest realizowane w ramach grantu w projekcie grantowym **„Cyberbezpieczny Samorząd”** współfinansowanym przez Unię Europejską z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: *Zaawansowane usługi cyfrowe*, Działanie 2.2. – *Wzmocnienie krajowego systemu cyberbezpieczeństwa*, na podstawie umowy o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/1613/ FERC.02.02-CS.01-001/23/2024 z dnia 3 lipca 2024 r. W ramach projektu przewidziano dostawę UTM, UPS i serwerów do kopii zapasowych wraz z dyskami dla Starostwa Powiatowego w Choszcznie i 5 jednostek organizacyjnych.

3. Tryb udzielenia zamówienia

1. Do niniejszego postępowania nie stosuje się przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień Publicznych (Dz. U. z 2023 r. poz. 1605 ze zm.) zgodnie z art. 2 ust. 1 pkt 1 ustawy.
2. Niniejsze postępowanie prowadzone jest w formie zapytania ofertowego

w oparciu o zasadę konkurencyjności o której mowa w podrozdziale 3.2 Wytycznych dotyczących kwalifikowalności wydatków na lata 2021-2027.

3. **Postępowanie prowadzone jest w języku polskim, poprzez Bazę Konkurencyjności (Aplikacja BK2021**): https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/
4. Oznaczenie wg Wspólnego Słownika Zamówień (kod CPV):
   32420000-3 – Urządzenia sieciowe,
   31154000-0 – Bezprzestojowe źródła energii,
   30233000-1 – Urządzenia do przechowywania i odczytu danych.
5. Zamawiający nie dopuszcza składania ofert częściowych.
6. Zamawiający nie dopuszcza składania ofert wariantowych.
7. Zamawiający nie przewiduje udzielania zamówień uzupełniających.

4. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawę UTM, UPS i serwerów do kopii zapasowych wraz z dyskami dla Starostwa Powiatowego w Choszcznie (**SP**) i 5 jednostek organizacyjnych:

1. Powiatowym Centrum Pomocy Rodzinie w Choszcznie (**PCPR**),
2. Powiatowym Zarządzie Dróg w Choszcznie (**PZD**),
3. Poradni Psychologiczno-Pedagogicznej w Choszcznie (**PPP**),
4. Domu Pomocy Społecznej w Brzezinach (**DPS**),
5. Specjalnym Ośrodku Szkolno-Wychowawczym im. Kawalerów Orderu Uśmiechu w Suliszewie (**SOSW**).

Przedmiot zamówienia obejmuje dostawę:

a) UTM z licencjami wsparcia – 3 szt.,
b) UPS – 42 szt.,
c) serwerów do kopii zapasowych – 4 szt.,
d) dysków twardych do macierzy dyskowej – 18 szt.

Przedmiot zamówienia obejmuje również instalację, konfigurację, uruchomienie, strojenie i wdrożenie oraz instruktaże z obsługi, a także serwis dostarczanych urządzeń.

4.1. Wymagania ogólne

1. Miejscem realizacji zamówienia jest siedziba Starostwa Powiatowego w Choszcznie (SP), ul. Nadbrzeżna 2, 73-200 Choszczno i odpowiednio jednostek organizacyjnych:
   1.1. PCPR – Powiatowe Centrum Pomocy Rodzinie, ul. Bolesława

Chrobrego 27a, 73-200 Choszczno

1.2. PZD – Powiatowy Zarząd Dróg, ul. Bolesława Chrobrego 27a, 73-200 Choszczno

1.3. PPP – Poradnia Psychologiczno-Pedagogiczna, ul. Bolesława Chrobrego 27, 73-200 Choszczno

1.4. DPS – Dom Pomocy Społecznej, Brzeziny 1, 73-220 Drawno

1.5. SOSW – Specjalny Ośrodek Szkolno- Wychowawczy w Suliszewie, ul. Zwycięstwa 28, 73-222 Suliszewo

2. Wykonawca w ramach realizacji zamówienia przygotuje szczegółowy program dostaw i przedstawi go Zamawiającemu w terminie w terminie nie później niż 7 dni roboczych od podpisania umowy na realizację zamówienia.
3. Przy realizacji zamówienia muszą zostać zachowane zasady równości szans i niedyskryminacji, w tym dostępność dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn. Jakiekolwiek produkty (w tym dokumentacja) muszą być zgodne z zasadami uniwersalnego projektowania oraz standardami równościowymi, w szczególności ze standardem cyfrowym.
4. Dokumentacja musi być dostosowana do potrzeb uczestników (np. posiadać możliwość powiększania treści), jeśli występują wśród nich osoby ze szczególnymi potrzebami. Jeśli potrzeby takie nie wystąpią, Zamawiający dopuszcza dostarczenie kompletu materiałów w formacie PDF.
5. Wykonawca zamówienia będzie zobowiązany do podpisania oświadczenia potwierdzającego przestrzeganie powyższych zasad.
6. Aby zachować regułę konkurencyjności dopuszcza się rozwiązania równoważne do rozwiązań wyspecyfikowanych przez Zamawiającego. Za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii, funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły, itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób. Za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt

systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, identycznych dla obu rozwiązań, dla których to warunków rozwiązania te są dedykowane.

7. W niniejszym dokumencie opisano wymagane parametry minimalne urządzeń, oprogramowania i usług. Wykonawca ma prawo zaoferować sprzęt i oprogramowanie o lepszych parametrach technicznych oraz szerszy zakres usług lub usługi o wyższym standardzie.
8. Dostarczane urządzenia i oprogramowanie muszą być sprawne, dobrej jakości i fabrycznie nowe. Dostarczony sprzęt nie może posiadać wad fizycznych i prawnych oraz musi być gotów do użytkowania bez żadnych dodatkowych zakupów i inwestycji. Pod pojęciem „fabrycznie nowe" Zamawiający rozumie produkty wykonane z nowych, nieregenerowanych elementów, bez śladów uszkodzenia, nie poleasingowe, posiadające zgodne z właściwymi przepisami atesty, certyfikaty, licencje i dopuszczenia, w oryginalnych opakowaniach (pojemnikach, obudowach) stosowanych typowo dla danego produktu przez producenta, zaopatrzone w etykiety identyfikujące dany produkt.
9. Dostarczane urządzenia muszą być wyprodukowane nie wcześniej niż 6 miesięcy przed terminem dostawy i nie mogą być uprzednio wykorzystywane lub prezentowane podczas wystaw lub prezentacji.
10. Dostarczane urządzenia muszą pochodzić z legalnego kanału dystrybucji w Unii Europejskiej, nieograniczającego uprawnień Zamawiającego do gwarancji producenta. Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
11. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (tekst jednolity Dz.U. 2023 poz. 1582) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
12. Producentami ani beneficjentami rzeczywistymi producentów oferowanego

sprzętu i oprogramowania nie mogą być firmy wpisane na listę osób i podmiotów, o której mowa w art. 2 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (tekst jednolity Dz.U. 2024 poz. 507).

13. Zamawiający zastrzega sobie prawo sprawdzenia, czy dostarczane urządzenia spełniają warunki wymienione w punktach 8. – 12. na wszelkie możliwe sposoby w dowolnym momencie realizacji zamówienia.

4.2. Wymagania dotyczące gwarancji

1. Zamawiający wymaga dla wszystkich dostarczanych urządzeń gwarancji i wsparcia serwisowego ich producentów lub autoryzowanych partnerów serwisowych. Kontakt z producentem będzie odbywał się przez Wykonawcę.
2. Gwarancja na sprzęt i oprogramowanie zostanie udzielona na okres wskazany w rozdziale 4.3 Specyfikacja techniczna, na następujących warunkach:
   a) Firma serwisująca musi posiadać certyfikat w zakresie zarządzania jakością stwierdzający zgodność z normą PN-EN ISO 9001:2015 na świadczenie usług serwisowych oraz, jeśli nie jest producentem, posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

   b) Serwis gwarancyjny świadczony będzie w miejscu użytkowania sprzętu, w obecności przedstawiciela Zamawiającego lub jeśli naprawa w siedzibie Zamawiającego nie jest możliwa, przedstawiciel służb serwisowych odbierze sprzęt i dostarczy po naprawie na własny koszt i na własną odpowiedzialność.

   c) Na czas naprawy poza siedzibą Zamawiającego sprzęt będzie zabierany bez dysku twardego, który zostanie wymontowany przez przedstawiciela Zamawiającego lub Wykonawcy. Po zwrocie naprawionego sprzętu dysk twardy zostanie ponownie zamontowany przez przedstawiciela Zamawiającego lub Wykonawcy, po czym nastąpi sprawdzenie poprawności funkcjonowania naprawionego sprzętu.

   d) Serwis gwarancyjny będzie świadczony w dni robocze od godziny 8:00 do 16:00.

   e) W przypadku zgłoszenia przez Zamawiającego awarii sprzętu, procedura naprawcza rozpocznie się w ciągu **maksimum jednego dnia roboczego**, licząc od momentu otrzymania zgłoszenia. W przypadku zgłoszenia otrzymanego po godzinie 15:00, czas reakcji liczy się od godziny 8.00 następnego dnia roboczego.

f) Naprawa serwisowa zostanie dokonana po uprzedniej nieodpłatnej ocenie zgłoszonej awarii. Ocena zgłoszonej awarii musi zostać dokonana przez wykwalifikowanego przedstawiciela służb serwisowych, w miejscu użytkowania sprzętu.

g) W celu przystąpienia do naprawy przedstawiciel służb serwisowych zgłosi się do miejsca użytkowania sprzętu.

h) Czas skutecznej naprawy sprzętu **nie może przekroczyć 3 dni roboczych**, licząc od momentu zgłoszenia awarii przez Zamawiającego.

i) W przypadku braku możliwości dotrzymania terminu skutecznej naprawy, określonego w lit. h, przedstawiciel służb serwisowych dostarczy i zainstaluje sprzęt zastępczy o nie gorszych parametrach niż urządzenie naprawiane. Po zakończeniu naprawy przedstawiciel służb serwisowych odbierze sprzęt zastępczy.

j) W razie, gdy czas naprawy sprzętu będzie dłuższy niż określony w lit. h, okres świadczenia gwarancji przedłuża się o czas trwania naprawy. W razie, gdy naprawa sprzętu potrwa dłużej niż 2 tygodnie, lub gdy sprzęt po raz trzeci ulegnie awarii podlegającej naprawie w ramach serwisu gwarancyjnego, Zamawiającemu będzie przysługiwało prawo do wymiany sprzętu na nowy; taki sam lub odpowiedni o nie gorszych parametrach.

k) Sprzęt zgłoszony przez Zamawiającego do naprawy przed upływem terminu gwarancji, podlega naprawie na zasadach serwisu gwarancyjnego.

3. W ramach udzielonej gwarancji Zamawiający oczekuje usunięcia wszelkich wad dostarczonego przedmiotu zamówienia, choćby takich jak np. wady techniczne, technologiczne, programowe i wykonawcze, uniemożliwiające prawidłową pracę lub obniżających jakość sprzętu.
4. Odpowiedzialność z tytułu gwarancji obejmuje zarówno wady powstałe z przyczyn tkwiących w przedmiocie umowy w chwili dokonania odbioru przez Zamawiającego, jak i wszelkie inne wady fizyczne powstałe z przyczyn, za które Zamawiający nie ponosi odpowiedzialności, pod warunkiem że wady te ujawnią się w okresie gwarancji.
5. Wykonawca udzieli rozszerzonej rękojmi za wady przedmiotu umowy w okresie równym okresowi gwarancji. Zamawiający może wykonywać uprawnienia z tytułu gwarancji niezależnie od uprawnień wynikających z rękojmi .
6. Za wadę fizyczną przedmiotu umowy, obok definicji wynikającej z Kodeksu cywilnego, należy rozumieć także jakąkolwiek niezgodność przedmiotu

dostawy z SOPZ.

4.3. Specyfikacja techniczna

W celu uzupełnienia posiadanej już przez SP i jednostki organizacyjne infrastruktury cyberbezpieczeństwa Wykonawca zobowiązany będzie do dostarczenia do odpowiednich lokalizacji następującego sprzętu:

a) dostawa UTM z licencjami wsparcia – 3 szt.

Dostawa systemu firewall/zaawansowanego UTM, pozwalającego na kontrolę ruchu wchodzącego i wychodzącego z sieci jednostek, analizę przesłanych pakietów pod względem ich treści oraz blokady znanych ataków i wykrywanie włamań lub ich prób do sieci wewnętrznych za pomocą IDS/IPS poprzez zaawansowaną technologię zapewniającą bezpieczeństwo sieci przed infekcjami. Oczekiwanym efektem jest zwiększenie bezpieczeństwa systemu, bezpieczna komunikacja jednostek z zewnętrznymi usługami sieciowymi, sprawne zarządzanie ruchem w sieciach informatycznych oraz zabezpieczenie ich przed wirusami, spamem i nieprawidłową treścią.

Dostawa obejmuje:

- UTM typu I – 2 szt.
- UTM typu II – 1 szt.

Dostawa ma zostać zrealizowana w do lokalizacji:

- SP – 2 szt. UTM typu I
- DPS – 1 szt. UTM typu II

Parametry sprzętu:

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
***** UTM typu I *****		
1.	Wymagania ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: – Firewall, – Ochrony w warstwie aplikacji, – Protokołów routingu dynamicznego.
2.	Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
3.	Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: – 10 portami Gigabit Ethernet RJ-45, – 2 gniazdami SFP 1 Gb/s. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Cyberbezpieczny Samorząd

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		3. System jest wyposażony w zasilanie AC.
4.	Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 1,4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gb/s dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,7 Gb/s. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gb/s. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix – minimum 1,3 Gb/s. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus – minimum 900 Mb/s. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mb/s.
5.	Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: – Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. – Kontrola Aplikacji. – Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. – Ochrona przed malware. – Ochrona przed atakami - Intrusion Prevention System. – Kontrola stron WWW. – Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. – Zarządzanie pasmem (QoS, Traffic shaping). – Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). – Dwuskładnikowe uwierzytelnianie z wykorzystaniem

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. – Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. – Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. – Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
6.	Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: – Translację jeden do jeden oraz jeden do wielu. – Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. – Amazon Web Services (AWS). – Microsoft Azure. – Cisco ACI. – Google Cloud Platform (GCP). – OpenStack. – VMware NSX. – Kubernetes.
7.	Połączenia VPN	System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: 1. Wsparcie dla IKE v1 oraz v2. 2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). 3. Obsługa protokołu Diffie-Hellman grup 19, 20. 4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. 5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. 7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. 8. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. 9. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. 10. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. 11. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. 12. Mechanizm „Split tunneling” dla połączeń Client-to-Site.

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: 1. Pracę w trybie Portal – gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. 2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. 3. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
8.	Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
9.	Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
10.	Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
11.	Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. 11. Możliwość rozbudowania Systemu o dodatkową funkcjonalność wstrzymania dostarczenia pliku, dla którego jest realizowana analiza z wykorzystaniem systemu Sandbox, do czasu otrzymania werdyktu z systemu Sandbox.
12.	Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
13.	Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
14.	Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak:

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
15.	Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia 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. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
16.	Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
17.	Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG.

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
18.	Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
19.	Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych – co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.
20.	Gwarancja oraz wsparcie	System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
21.	Dodatkowe wymagania	1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym. 3. Zamawiający wymaga, aby wsparcie serwisowe świadczył zespół (minimum 2 osoby) certyfikowanych inżynierów w zakresie administracji systemami UTM, legitymujący się ważnymi certyfikatami Certified Professional Network Security. 4. Wykonawca przedstawi oświadczanie o gotowości świadczenia wymaganego serwisu zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej. 5. Wykonawca załączy do oferty certyfikat ISO 27001 na projektowanie sprzedaż i wdrażanie rozwiązań teleinformatycznych, świadczenie usług serwisowych i konsultingowych.
22.	Liczba sztuk	Zamawiający wymaga dostarczenia 2 sztuk UTM typu I.

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		***** UTM typu II *****
1.	Wymagania ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: – Firewall, – Ochrony w warstwie aplikacji, – Protokołów routingu dynamicznego.
2.	Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		tworzenia interfejsów redundantnych.
3.	Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall dysponuje co najmniej 10 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System jest wyposażony w zasilanie AC.
4.	Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gb/s dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,7 Gb/s. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gb/s. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix – minimum 1,3 Gb/s. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus – minimum 650 Mb/s. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mb/s.
5.	Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: – Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. – Kontrola Aplikacji. – Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. – Ochrona przed malware.

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		– Ochrona przed atakami - Intrusion Prevention System. – Kontrola stron WWW. – Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. – Zarządzanie pasmem (QoS, Traffic shaping). – Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). – Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. – Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. – Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. – Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
6.	Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: – Translację jeden do jeden oraz jeden do wielu. – Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. – Amazon Web Services (AWS). – Microsoft Azure. – Cisco ACI. – Google Cloud Platform (GCP). – OpenStack. – VMware NSX. – Kubernetes.
7.	Połączenia VPN	System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: 1. Wsparcie dla IKE v1 oraz v2. 2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). 3. Obsługa protokołu Diffie-Hellman grup 19, 20. 4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. 5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. 7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. 8. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. 9. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		ochrony zasobów systemu. 10. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. 11. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. 12. Mechanizm „Split tunneling” dla połączeń Client-to-Site. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: 1. Pracę w trybie Portal – gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. 2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. 3. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
8.	Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
9.	Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
10.	Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
11.	Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
12.	Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
13.	Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
14.	Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia 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. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
15.	Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
16.	Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
17.	Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
18.	Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych – co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.
19.	Gwarancja oraz wsparcie	System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
20.	Dodatkowe wymagania	1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym. 3. Zamawiający wymaga, aby wsparcie serwisowe świadczył zespół (minimum 2 osoby) certyfikowanych inżynierów w zakresie administracji systemami UTM, legitymujący się ważnymi certyfikatami Certified Professional Network Security. 4. Wykonawca przedstawi oświadczanie o gotowości świadczenia wymaganego serwisu zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej. 5. Wykonawca załączy do oferty certyfikat ISO 27001 na projektowanie sprzedaż i wdrażanie rozwiązań teleinformatycznych, świadczenie usług serwisowych i konsultingowych.
21.	Liczba sztuk	Zamawiający wymaga dostarczenia 1 sztuki UTM typu II.

b) dostawa UPS – 42 szt.

Dostawa zasilaczy awaryjnych (urządzeń typu UPS rack i UPS) do zabezpieczenia przed zanikiem napięcia na urządzeniach sieciowych, serwerach i komputerach stacjonarnych SP i jednostek organizacyjnych, które umożliwią nieprzerwaną, poprawną pracę w sieci informatycznej i zabezpieczyć te urządzenia przed uszkodzeniem.

Dostawa obejmuje:

- UPS typu I – 3 szt.
- UPS typu II – 1 szt.
- UPS typu III – 33 szt.
- UPS typu IV – 5 szt.

Dostawa ma zostać zrealizowana w do lokalizacji:

- SP – 2 szt. UPS typu I
- PCPR – 1 szt. UPS typu II, 13 szt. UPS typu III
- PPP – 10 szt. UPS typu III
- DPS – 1 szt. UPS typu I, 5 szt. UPS typu IV
- SOSW – 10 szt. UPS typu III

Parametry sprzętu:

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		***** UPS typu I *****
1.	Wymagania techniczne	1. Moc znamionowa jednostki nie mniej niż 1800W / 2000VA 2. Montowany w szafie RACK (komplet uchwytów w zestawie) 3. Technologia Double Conversion (On-Line) 4. Temperatura eksploatacji 0 - 40 °C 5. Wilgotność względna podczas pracy 0 - 95 % 6. Wysokość n.p.m. podczas pracy 0-3000m, powyżej 3000m n. p. m. następuje obniżenie wartości znamionowych 7. Hałas słyszalny w odległości 1 m od powierzchni urządzenia do 53.0dBA 8. Rozpraszanie ciepła w trybie online 759.0BTU/godz. 9. Klasa energetyczna sprzętu przeciwprzepięciowego 600 Dżuli 10. Możliwość zimnego startu 11. Automatyczne włączenie UPS-a po powrocie zasilania
2.	Parametry wejściowe	1. Nominalne napięcie wejściowe 220V, 230V, 240V 2. Zakres częstotliwości wejściowej: 40-70 Hz 3. Typ gniazda wejściowego: IEC-320 C14 4. Zmienny zakres napięcia wejściowego w trybie podstawowym 105- 300V
3.	Parametry	1. Napięcie wyjściowe 220V, 230V, 240V

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
	wyjściowe	2. Zniekształcenia napięcia poniżej 3% dla obciążeń liniowych oraz poniżej 6% dla obciążeń nieliniowych 3. Częstotliwość na wyjściu zsynchronizowana z siecią zasilającą 50/60 Hz (±3Hz dla zasilania z sieci lub ±0.1Hz dla zasilania z baterii) 4. Typ przebiegu sinusoida 5. Złącza/gniazda wyjściowe 4 szt. IEC 320 C13
4.	Akumulatory i czas podtrzymania	1. Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu 2. Czas autonomii pracy przy zasilaniu akumulatorowym: – 21 minut 55 sekund dla pełnego obciążenia – 51 minut dla połowy obciążenia 3. Typowy czas ładowania 4 godziny 4. Oczekiwana żywotność akumulatora (lata) 3 – 5 5. Automatyczny test akumulatora
5.	Komunikacja i zarządzanie	1. Porty komunikacyjne: RS-232 Serial, USB, Smart Slot (karta zarzadzania sieciowego SNMP sprzedawana oddzielnie) 2. Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD 3. Alarm dźwiękowy: Alarm przy zasilaniu z akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia 4. Złącze awaryjnego wyłączenia zasilania (EPO)
6.	Certyfikaty, zgodności oraz gwarancja	1. Znak CE, RoHS, REACH 2. 2 lata na naprawę lub wymianę
7.	Oprogramowanie	Dostępne oprogramowanie do zarządzania/monitorigu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®.
8.	Liczba sztuk	Zamawiający wymaga dostarczenia 3 sztuk UPS typu I.

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		***** UPS typu II *****
1.	Wymagania techniczne	1. Moc znamionowa jednostki nie mniej niż 750VA / 500W 2. Montaż w szafie Rack 3. Technologia Line Interactive 4. Temperatura eksploatacji 0 - 40 °C 5. Wilgotność względna podczas pracy 0 - 95 % 6. Wysokość n.p.m. podczas pracy 0-3000 m 7. Hałas słyszalny w odległości 1 m od powierzchni urządzenia 42,0 dBA 8. Rozpraszanie ciepła w trybie online 46,00 BTU/h 9. Klasa energetyczna sprzętu przeciwprzepięciowego 459J
2.	Parametry wejściowe	1. Nominalne napięcie wejściowe 230V 2. Częstotliwość wejściowa 50/60 Hz +/-3 Hz (automatyczne wykrywanie) 3. Typ gniazda wejściowego: IEC-320 C14 4. Zmienny zakres napięcia wejściowego w trybie podstawowym 160 - 286V 5. Inne napięcia wejściowe 220, 240
3.	Parametry wyjściowe	1. Napięcie wyjściowe 230VAC 2. Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz +/- 3 Hz 3. Inne napięcia wyjściowe 220, 240 4. Typ przebiegu sinusoida 5. Złącza/gniazda wyjściowe 6. (4) IEC 320 C13
4.	Akumulatory i czas podtrzymania	1. Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu 2. Czas autonomii: – 5 minuty 27 sekundy dla pełnego obciążenia – 16 minut 4 sekundy dla połowy obciążenia 3. Typowy czas ładowania 3 godziny 4. Oczekiwana żywotność akumulatora (lata) 3 – 5 5. Baterie wymieniane na gorąco
5.	Komunikacja i zarządzanie	1. Gniazdo do montażu karty WEB/SNMP- Smart Slot x1 2. Moduł WEB/SNMP obsługiwane protokoły komunikacyjne:

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		– IP v.6 – SNMP v.3 – Modbus TCP 3. Porty komunikacyjne: RJ-45 Serial, SmartSlot, USB 4. Panel sterowania: – Wielofunkcyjna konsola sterownicza i informacyjna LCD – Alarm dźwiękowy: Alarm przy zasilaniu akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia
6.	Certyfikaty, zgodności oraz gwarancja	1. CSA, EAC, EN/IEC 62040-1, EN/IEC 62040-2, RCM, UL 1778, VDE, RoHS 2. 3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulator
7.	Oprogramowanie	Oprogramowanie do zarządzania zasilaczami UPS do bezpiecznego wyłączania i zarządzania energią dla komputerów stacjonarnych, serwerów i stacji roboczych, wykorzystujące dedykowane połączenia szeregowe lub USB i oferujące: – Monitorowania i zarządzania zasilaczy UPS – Bezobsługowego, bezpiecznego wyłączania podczas problemów z zasilaniem – Bezpieczny dostęp do internetowego interfejsu użytkownika (UI) – Możliwość dokładnego określania czasu i sekwencji zdarzeń powodujących zdarzenie za pomocą dziennika zdarzeń – Identyfikację potencjalnie niebezpiecznych trendów zanim dojdzie do eskalacji problemu lub eksportowanie dziennika w celu analizy
8.	Liczba sztuk	Zamawiający wymaga dostarczenia 1 sztuki UPS typu II.

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
*** UPS typu III ***		
1.	Wymagania techniczne	1. Moc znamionowa jednostki nie mniej niż 520W / 950VA 2. Topologia line-interactive 3. Temperatura eksploatacji 0 - 40 °C 4. Wilgotność względna podczas pracy 0 - 90 % 5. Wysokość n.p.m. podczas pracy 0-3000 m 6. Klasa energetyczna sprzętu przeciwprzepięciowego 273 Dżule 7. Zabezpieczenie przeciwprzepięciowe: bezpiecznik minimum 7A
2.	Parametry wejściowe	1. Nominalne napięcie wejściowe 230V 2. Częstotliwość wejściowa 50/60 Hz +/-5 Hz (automatyczne wykrywanie) 3. Standard wtyczki: IEC 60320 C13
3.	Parametry wyjściowe	1. Napięcie wyjściowe 230V 2. Zniekształcenia napięcia wyjściowego +/- 10% 3. Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz +/- 3 Hz 4. Power factor: minimum 0.55 5. Typ przebiegu: Schodkowa aproksymacja sinusoidy 6. Złącza/gniazda wyjściowe: – 6 gniazd IEC 60320 C13 z zabezpieczeniem przeciwprzepięciowym oraz podtrzymaniem zasilania. 7. 1 gniazdo USB-B (komunikacyjne)
4.	Akumulatory i czas podtrzymania	1. Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu 2. Czas autonomii: – 29 sekund dla pełnego obciążenia – 6 minut 42 sekundy dla połowy obciążenia 3. Typowy czas ładowania 6-8 godzin 4. Oczekiwana żywotność akumulatora (lata) 2 – 5
5.	Komunikacja i zarządzanie	1. Gniazdo RJ45 Gigabit 2. Diody LED wskazująca na status zasilania: zasilanie z sieci energetycznej : zasilanie z akumulatora 3. Alarm dźwiękowy: Praca na baterii, niski poziom naładowania baterii, wyłączenie baterii, zastępcza

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		bateria wykryta
6.	Certyfikaty, zgodności oraz gwarancja	1. Znak CE CB, EAC 2. EN/IEC 62040-1:2019/A11:2021 3. EN/IEC 62040-2:2006/AC:2006 4. EN/IEC 62040-2:2018 5. 2 lata na naprawę lub wymianę, 3 lata gwarancji naprawy lub wymiany w krajach Unii Europejskiej
7.	Oprogramowanie	Oprogramowanie do zarządzania zasilaczami UPS do bezpiecznego wyłączania i zarządzania energią dla komputerów stacjonarnych, serwerów i stacji roboczych, wykorzystujące dedykowane połączenia szeregowe lub USB i oferujące: – Monitorowania i zarządzania zasilaczy UPS – Bezobsługowego, bezpiecznego wyłączania podczas problemów z zasilaniem – Bezpieczny dostęp do internetowego interfejsu użytkownika (UI) – Możliwość dokładnego określania czasu i sekwencji zdarzeń powodujących zdarzenie za pomocą dziennika zdarzeń – Identyfikację potencjalnie niebezpiecznych trendów zanim dojdzie do eskalacji problemu lub eksportowanie dziennika w celu analizy
8.	Liczba sztuk	Zamawiający wymaga dostarczenia 33 sztuk UPS typu III.

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		***** UPS typu IV *****
1.	Wymagania techniczne	1. Moc znamionowa jednostki nie mniej niż 865W / 1500VA 2. Topologia line-interactive 3. Temperatura eksploatacji 0 - 40 °C 4. Wilgotność względna podczas pracy 0 - 95 % 5. Wysokość n.p.m. podczas pracy 0-3000 m 6. Klasa energetyczna sprzętu przeciwprzepięciowego 441 Dżuli 7. Zabezpieczenie przeciwprzepięciowe: bezpiecznik minimum 10A

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
2.	Parametry wejściowe	1. Nominalne napięcie wejściowe 230V 2. Częstotliwość wejściowa 50/60 Hz +/-3 Hz (automatyczne wykrywanie) 3. Standard wtyczki: francuska/belgijska
3.	Parametry wyjściowe	1. Napięcie wyjściowe 230V 2. Inne napięcia wyjściowe 196V-264V 3. Zniekształcenia napięcia wyjściowego +/- 8% 4. Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz +/- 1 Hz 5. Power factor: minimum 0.58 6. Typ przebiegu: Schodkowa aproksymacja sinusoidy 7. Złącza/gniazda wyjściowe: – 3 gniazda francuska/belgijska z zabezpieczeniem przeciwprzepięciowym oraz podtrzymaniem zasilania, 8. 3 gniazda francuska/belgijska z zabezpieczeniem przeciwprzepięciowym
4.	Akumulatory i czas podtrzymania	1. Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu 2. Czas autonomii: – 3 minuty 39 sekund dla pełnego obciążenia – 10 minut 30 sekund dla połowy obciążenia 3. Typowy czas ładowania 12 godzin 4. Oczekiwana żywotność akumulatora (lata) 3 – 5
5.	Komunikacja i zarządzanie	1. Gniazda RJ45 (Gigabit), RJ11, USB/Serial 2. Diody LED wskazująca na status zasilania: zasilanie z sieci energetycznej: zasilanie z akumulatora 3. Alarm dźwiękowy: Praca na baterii, niski poziom naładowania baterii, wyłączenie baterii, zastępcza bateria wykryta
6.	Certyfikaty, zgodności oraz gwarancja	1. Znak CE 2. EN/IEC 62040-1:2019/A11:2021 3. EN/IEC 62040-2:2006/AC:2006 4. EN/IEC 62040-2:2018 5. 2 lata na naprawę lub wymianę, 3 lata gwarancji naprawy lub wymiany w krajach Unii Europejskiej
7.	Oprogramowanie	Oprogramowanie do zarządzania zasilaczami UPS do

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		bezpiecznego wyłączania i zarządzania energią dla komputerów stacjonarnych, serwerów i stacji roboczych, wykorzystujące dedykowane połączenia szeregowe lub USB i oferujące: – Monitorowania i zarządzania zasilaczy UPS – Bezobsługowego, bezpiecznego wyłączania podczas problemów z zasilaniem – Bezpieczny dostęp do internetowego interfejsu użytkownika (UI) – Możliwość dokładnego określania czasu i sekwencji zdarzeń powodujących zdarzenie za pomocą dziennika zdarzeń – Identyfikację potencjalnie niebezpiecznych trendów zanim dojdzie do eskalacji problemu lub eksportowanie dziennika w celu analizy
8.	Liczba sztuk	Zamawiający wymaga dostarczenia 5 sztuk UPS typu IV.

c) dostawa serwerów do kopii zapasowych – 4 szt.

Dostawa systemu kopii zapasowych (macierzy NAS), który pozwoli na łatwe odzyskanie danych z serwera produkcyjnego oraz na utrzymanie ciągłości pracy. Stworzony ma zostać dedykowany system odmiejscowionej kopii zapasowej pozwalającej na odtworzenie kompletnego systemu. Na dedykowanym serwerze zostanie zainstalowane oprogramowanie do backupu i archiwizacji danych. Miejscem przechowywania danych backupu będą dyski serwera.

Dostawa obejmuje:

- serwer typu I – 1 szt.
- serwer typu II – 3 szt.

Dostawa ma zostać zrealizowana w do lokalizacji:

- SP – 1 szt. serwera typu II
- PCPR – 1 szt. serwera typu II
- PPP – 1 szt. serwera typu II
- SOSW – 1 szt. Serwera typu I

Parametry sprzętu:

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
*** Serwer typu I ***		
1.	Procesor	Procesor 4 rdzeniowy 64 bit x86 o taktowaniu nie mniejszym niż 2.2 GHz
2.	Pamięć RAM	Nie mniej niż 8GB z możliwością rozszerzenia do 64GB
3.	Pamięć Flash	Nie mniej niż 5GB
4.	Obudowa	Tower, z obsługa min. 4 dysków 3,5” SATA HDD oraz 2,5” SATA HDD/SSD, 2 dysków M.2 PCIe Gen3
5.	Dyski twarde	1. Zainstalowane 4 dyski o pojemności min. 8TB każdy 2. Możliwość stosowania dysków o pojemności do 18TB 3. Możliwość zwiększenia ilości obsługiwanych dysków za pomocą nie mniej niż 2 modułów rozszerzających.
6.	Komunikacja sieciowa	1. Min. 2 porty RJ-45 o prędkości 2,5GbE, z możliwością agregacji. 2. Możliwość podłączenia karty WLAN na USB
7.	Porty USB	Min. 3 porty USB 3.2 Gen 2
8.	Porty wewnętrzne	Min. 2 porty PCIe Gen3 x4
9.	Zasilacz	Max. 250W
10.	Obsługa dwóch systemów operacyjnych	Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS
11.	Obsługiwane systemy plików	1. Dyski wewnętrzne: EXT4 2. Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT
12.	Szyfrowanie	1. Min. AES 256, 2. Możliwość szyfrowania dysków zewnętrznych.
13.	Zarządzanie dyskami	1. Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, 2. Obsługa Hot Spare per grupa RAID oraz global hot spare 3. Rozszerzanie pojemności Online RAID 4. Migracja poziomów Online RAID 5. HDD S.M.A.R.T. 6. Skanowanie uszkodzonych bloków 7. Przywracanie macierzy RAID 8. Obsługa map bitowych 9. Pula pamięci masowej 10. Obsługa migawek 11. Obsługa replikacji migawek

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
14.	Wbudowana obsługa iSCSI	1. Multi-LUNs na Target 2. Obsługa LUN Mapping & Masking 3. Obsługa SPC-3 Persistent Reservation 4. Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
15.	Obsługiwane serwery	1. Serwer plików 2. Serwer FTP 3. Serwer WEB 4. Serwer kopii zapasowych 5. Serwer multimediów UPnP 6. Serwer pobierania (Bittorrent / HTTP / FTP) 7. Serwer Monitoringu
16.	VPN	1. VPN client / VPN server 2. Obsługa PPTP 3. OpenVPN
17.	Administracja systemu	1. Połączenia HTTP/HTTPS 2. Powiadamianie przez e-mail (uwierzytelnianie SMTP) 3. Powiadamianie przez SMS 4. Ustawienia inteligentnego chłodzenia 5. DDNS oraz zdalny dostęp w chmurze 6. SNMP (v2 & v3) 7. Obsługa UPS z zarządzaniem SNMP (USB) 8. Obsługa sieciowej jednostki UPS 9. Monitor zasobów 10. Kosz sieciowy dla CIFS/SMB oraz AFP 11. Monitor zasobów systemu w czasie rzeczywistym 12. Rejestr zdarzeń 13. System plików dziennika 14. Całkowity rejestr systemowy (poziom pliku) 15. Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line 16. Aktualizacja oprogramowania automatyczna 17. Możliwość aktualizacji oprogramowania ręcznie 18. Ustawienia systemu: Kopia, Przywracanie, Resetowanie
18.	Wirtualizacja	1. Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android.

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		2. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 3. Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
19.	Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
20.	Zabezpieczenia	1. Filtracja IP 2. Ochrona dostępu do sieci z automatycznym blokowaniem 3. Połączenie HTTPS 4. FTP z SSL/TLS (Explicit) 5. Obsługa SFTP (tylko admin) 6. Szyfrowanie AES 256-bit 7. Szyfrowana zdalna replikacja (Rsync poprzez SSH) 8. Import certyfikatu SSL 9. Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
21.	Możliwość instalacji dodatkowego oprogramowania	1. sklep z aplikacjami 2. możliwość instalacji z paczek
22.	Gwarancja	36 miesięcy
23.	Liczba sztuk	Zamawiający wymaga dostarczenia 1 sztuki serwera typu I.

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
*** Serwer typu II ***		
1.	Procesor	Procesor 4 rdzeniowy 32 bit x86 o taktowaniu nie mniejszym niż 1.7 GHz
2.	Pamięć RAM	Nie mniej niż 8GB
3.	Pamięć Flash	Nie mniej niż 512MB
4.	Obudowa	RACK 1U, z obsługa min. 4 dysków 3,5” SATA HDD oraz 2,5” SATA HDD/SSD
5.	Zainstalowane dyski twarde	Zgodnie z opisem w punkcie d)
6.	Obsługiwane dyski twarde	Możliwość stosowania dysków o pojemności do 24TB
7.	Komunikacja sieciowa	1. Min. 2 porty RJ-45 o prędkości 1GbE, z możliwością agregacji. 2. Min. 1 port SFP+ o prędkości 10GbE 3. Możliwość podłączenia karty WLAN na USB
8.	Porty USB	Min. 4 porty USB 3.2 Gen 2
9.	Zasilacz	Min. 100W
10.	Obsługiwane systemy plików	1. Dyski wewnętrzne: EXT4 2. Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
11.	Szyfrowanie	1. Min. AES 256, 2. Możliwość szyfrowania dysków zewnętrznych.
12.	Zarządzanie dyskami	1. Pojedynczy Dysk, RAID 0,1, 5, 6, 10, 5+Hot Spare 2. Rozszerzanie pojemności Online RAID 3. Migracja poziomów Online RAID 4. HDD S.M.A.R.T. 5. Skanowanie uszkodzonych bloków (pliku) 6. Przywracanie macierzy RAID 7. Obsługa map bitowych 8. Globalny Hot Spare, Pula pamięci masowej
13.	Wbudowana obsługa iSCSI	1. Multi-LUNs na Target 2. Obsługa LUN Mapping & Masking 3. Obsługa SPC-3 Persistent Reservation 4. Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
14.	Zarządzanie prawami dostępu	1. Ograniczenie dostępnej pojemności dysku dla użytkownika 2. Importowanie listy użytkowników

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		3. Zarządzanie kontami użytkowników 4. Zarządzanie grupą użytkowników 5. Zarządzanie współdzieleniem w sieci 6. Tworzenie użytkowników za pomocą makr 7. Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
15.	Obsługa Windows AD	1. Logowanie użytkowników do domeny poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web 2. Funkcja serwera LDAP
16.	Funkcje backup	1. Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, 2. Backup na zewnętrzne dyski twarde.
17.	Współpraca z zewnętrznymi dostawcami usług chmury	1. Amazon S3, 2. Amazon Glacier, 3. Microsoft Azure, 4. Google Cloud Storage, 5. Dropbox.
18.	Darmowe aplikacje na urządzenia mobilne	1. Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki 2. Dostępne na systemy iOS oraz Android
19.	Obsługiwane serwery	1. Serwer plików 2. Serwer FTP 3. Serwer WEB 4. Serwer baz danych MySQL 5. Serwer kopii zapasowych 6. Serwer multimediów UPnP 7. Serwer pobierania (Bittorrent / HTTP / FTP) 8. Serwer Monitoringu
20.	VPN	1. VPN client / VPN server 2. Obsługa PPTP 3. OpenVPN 4. L2TP
21.	Administracja systemu	1. Połączenia HTTP/HTTPS 2. Powiadamianie przez e-mail (uwierzytelnianie SMTP) 3. Powiadamianie przez SMS 4. DDNS oraz zdalny dostęp w chmurze

Lp.	Nazwa cechy / komponentu	Minimalne parametry techniczne
		5. SNMP (v2 & v3) 6. Obsługa UPS z zarządzaniem SNMP (USB) 7. Obsługa sieciowej jednostki UPS 8. Monitor zasobów 9. Kosz sieciowy dla CIFS/SMB oraz AFP 10. Monitor zasobów systemu w czasie rzeczywistym 11. Rejestr zdarzeń 12. System plików dziennika 13. Całkowity rejestr systemowy (poziom pliku) 14. Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line 15. Aktualizacja oprogramowania 16. Możliwość ręcznej aktualizacji oprogramowania 17. Ustawienia: Back up, przywracania, resetowania systemu
22.	Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
23.	Zabezpieczenia	1. Filtracja IP 2. Ochrona dostępu do sieci z automatycznym blokowaniem 3. Połączenie HTTPS 4. FTP z SSL/TLS (Explicit) 5. Obsługa SFTP (tylko admin) 6. Szyfrowanie AES 256-bit 7. Szyfrowana zdalna replikacja (Rsync poprzez SSH) 8. Import certyfikatu SSL 9. Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
24.	Możliwość instalacji dodatkowego oprogramowania	1. sklep z aplikacjami 2. możliwość instalacji z paczek
25.	Gwarancja	36 miesięcy
26.	Liczba sztuk	Zamawiający wymaga dostarczenia 3 sztuk serwera typu II.

d) dostawa dysków twardych do macierzy dyskowej – 18 szt.

Dostawa dysków twardych do serwerów kopii zapasowych (macierzy NAS), dostarczanych w ramach punktu c) oraz do macierzy dyskowej w serwerze

funkcjonującym w PCPR (Dell PowerEdge T340, Service Tag: 265DG13).

Dyski mają zostać zamontowane w dostarczanych serwerach kopii zapasowych oraz we wskazanym serwerze. Dyski muszą współpracować z opisanym sprzętem.

Dostawa obejmuje:

- Dysk HDD serwerowy 8TB – 6 szt.
- Dysk HDD serwerowy 4TB – 12 szt.

Dostawa ma zostać zrealizowana w do lokalizacji:

- SP – 2 szt. dysków HDD serwerowych 8TB
- PCPR – 4 szt. dysków HDD serwerowych 8TB (do macierzy z punktu c) oraz 4 szt. dysków HDD serwerowych 4TB (do serwera Dell PowerEdge T340, Service Tag: 265DG13)
- PPP – 4 szt. dysków HDD serwerowych 8TB
- SOSW – 4 szt. dysków HDD serwerowych 8TB

5. Termin realizacji zamówienia

Zamówienie musi zostać zrealizowane w terminie: od daty podpisania umowy do 20 grudnia 2024 r.

6. Warunki płatności

Płatność po wykonaniu zamówienia.
Termin płatności – 30 dni od dnia dostarczenia do siedziby Zamawiającego poprawnie wystawionej faktury VAT.

7. Warunki udziału w postępowaniu

O udzielenie poszczególnych części zamówienia mogą ubiegać się Wykonawcy nie podlegający wykluczeniu i spełniający warunki udziału w postępowaniu, dotyczące **zdolności technicznej lub zawodowej**, którzy:

1) posiadają status autoryzowanego partnera producenta/-ów oferowanych w ramach zamówienia urządzeń UTM oraz serwerów do kopii zapasowych na poziomie uprawniającym do sprzedaży na terenie Polski, potwierdzony odpowiednim/-i certyfikatem/-ami producenta/-ów,
2) posiadają certyfikat ISO 27001:2017 na projektowanie, sprzedaż i wdrażanie rozwiązań teleinformatycznych,
3) w okresie ostatnich trzech lat przed terminem składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonali co najmniej 3

dostawy infrastruktury przetwarzania danych kopii zapasowych z usługą wdrożenia i wsparcia technicznego, na kwotę co najmniej 100 000,00 zł brutto każda,

4) na potrzeby realizacji zamówienia dysponuje lub będzie dysponował co najmniej 1 (jednym) specjalistą posiadającym uprawnienia (certyfikat) na poziomie Certified Professional Network Security w zakresie wdrażanych rozwiązań UTM, który dokona instalacji, uruchomienia i konfiguracji dostarczonych urządzeń.

Na potwierdzenie spełnienia ww. warunków Wykonawca zobowiązany jest przedstawić:

- **wykaz usług** zrealizowanych w okresie ostatnich trzech lat przed upływem terminu składania ofert wraz z dokumentami potwierdzającym należytą realizację zamówień (np. listy referencyjne, protokoły odbiorów bez uwag) – wzór wykazu stanowi **załącznik nr 2.** do niniejszego zapytania ofertowego.
- **wykaz osób** przeznaczonych do realizacji zamówienia publicznego, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień i doświadczenia niezbędnego do wykonania zamówienia, a także kopiami dokumentów potwierdzającymi posiadane doświadczenie i certyfikaty – wzór wykazu stanowi **załącznik nr 3.** do niniejszego zapytania ofertowego.

Oferty Wykonawców nie spełniających ww. warunków nie będą rozpatrywane.

Zamawiający zastrzega sobie prawo sprawdzania w toku oceny ofert wiarygodności przedstawionych przez Wykonawcę dokumentów, wykazów, danych i informacji.

8. Wykluczenie z udziału w postępowaniu

I. O udzielenie zamówienia nie może ubiegać się Wykonawca w stosunku do którego zachodzi którakolwiek z okoliczności, o których mowa w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2023 r. poz. 1497 z późn. zm.);

II. Zamawiający wykluczy z postępowania Wykonawcę, który jest powiązany z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a Wykonawcą, polegające w szczególności na:
    1. uczestniczeniu w spółce, jako wspólnik spółki cywilnej lub spółki

osobowej,
2. posiadaniu co najmniej 10% udziałów lub akcji,
3. pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
4. pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

9. Sposób przygotowania oferty

1. Ofertę należy sporządzić na formularzu ofertowym stanowiącym **załącznik nr 1.** do niniejszego zapytania ofertowego.
2. Do oferty musi zostać załączony wykaz usług stanowiący **załącznik nr 2.** do niniejszego zapytania ofertowego oraz wykaz osób przeznaczonych do realizacji zamówienia stanowiący **załącznik nr 3.**
3. Cena oferty musi być ceną ryczałtową, obejmować dowolną liczbę części zamówienia w całości i być podana w złotych polskich. Cena musi być rozbita na kwoty cząstkowe stanowiące wynagrodzenie za realizację poszczególnych części zamówienia.
4. Oferta winna być podpisana przez osobę/y upoważnione do reprezentowania Wykonawcy.
5. Ofertę należy podpisać podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu lub podpisem zaufanym.
6. Wykonawca ma prawo złożyć tylko 1 ofertę. Złożenie przez Wykonawcę więcej niż 1 oferty, skutkuje odrzuceniem wszystkich ofert złożonych przez tego Wykonawcę.
7. Wszelkie koszty przygotowania oferty ponosi Wykonawca.
8. Nie przewiduje się zwrotu kosztów udziału w postępowaniu.
9. Termin związania ofertą wynosi 30 dni.
10. Wykonawca informuje Zamawiającego o informacjach zawartych w ofercie stanowiących tajemnicę przedsiębiorstwa.

10. Wymagane dokumenty

Wraz z ofertą Wykonawca jest zobowiązany złożyć dokumenty potwierdzające należytą realizację zamówień wymienionych w wykazie usług oraz certyfikaty potwierdzające posiadanie przez audytorów uprawnień wymienione w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Fundusze Europejskie na Rozwój Cyfrowy

11. Miejsce i termin składania ofert:

1. Ofertę wraz z załącznikami należy złożyć za pośrednictwem portalu Baza Konkurencyjności – https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl **w terminie do dnia 28.11.2024 r. do godziny 10:00.**
2. O terminowym złożeniu oferty decyduje data złożenia oferty za pośrednictwem portalu Baza Konkurencyjności.
3. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
4. Ofertę wraz z załącznikami składa się, pod rygorem nieważności, w postaci elektronicznej **podpisanej kwalifikowanym podpisem elektronicznym** lub **podpisem zaufanym** przez osobę/y upoważnioną/e do reprezentowania wykonawcy. Brak podpisu/ów w wymieniony sposób będzie skutkował odrzuceniem oferty.
5. Oferta winna być sporządzona w języku polskim pod rygorem nieważności. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem przysięgłym na język polski.
6. **Zamawiający nie dopuszcza innej formy i sposobu składania ofert niż za pośrednictwem portalu Baza Konkurencyjności**. Niespełnienie tego wymogu oznacza niezgodność oferty z Zapytaniem. Oferty złożone w inny sposób zostaną odrzucone przez Zamawiającego.

12. Kryteria wyboru oferty

1. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:
   a) **cena brutto (C) – 70%**

   Zamawiający dokona przeliczenia cen ofert na punkty z dokładnością do dwóch miejsc po przecinku, według następującego wzoru:

$$\frac{\text{Najniższa cena spośród ofert nieodrzuconych}}{\text{Cena oferty badanej}} \times 100$$

   b) **termin realizacji zamówienia (T) – 30%**

   Zamawiający przyzna punkty w tym kryterium w następujący sposób:

   T = 0 pkt. – jeśli termin realizacji zamówienia wynosi 8 tygodni od daty podpisania umowy na realizację zamówienia,

   T = 5 pkt. – jeśli termin realizacji zamówienia wynosi nie więcej niż 7 tygodni od daty podpisania umowy na realizację zamówienia,

T = 15 pkt. – jeśli termin realizacji zamówienia wynosi nie więcej niż 6 tygodni od daty podpisania umowy na realizację zamówienia,

T = 30 pkt. – jeśli termin realizacji zamówienia wynosi nie więcej niż 4 tygodnie od daty podpisania umowy na realizację zamówienia.

UWAGA!

Wymaga się wpisania w formularzu terminu realizacji zamówienia w pełnych tygodniach. W przypadku podania terminu zamówienia w niepełnych tygodniach, liczba zostanie zaokrąglona do pełnych tygodni zgodnie z regułami matematycznymi.

Minimalny termin realizacji zamówienia, jaki może zaoferować Wykonawca, to 4 tygodnie od daty podpisania umowy na realizację zamówienia, maksymalny termin realizacji, jaki może zaoferować Wykonawca, to 8 tygodni od daty podpisania umowy na realizację zamówienia.

W przypadku gdy Wykonawca zaproponuje termin realizacji zamówienia dłuższy niż 8 tygodni od daty podpisania umowy na realizację zamówienia jego oferta zostanie odrzucona jako niezgodna z SWZ.

W przypadku gdy Wykonawca zaproponuje termin realizacji zamówienia krótszy niż 4 tygodnie od daty podpisania umowy na realizację zamówienia do celu oceny ofert Zamawiający przyjmie, że Wykonawca wpisał 4 tygodnie od daty podpisania umowy na realizację zamówienia, jednak do umowy zostanie wpisana liczba tygodni podana w ofercie.

W przypadku niewpisania w ofercie terminu realizacji zamówienia (liczby tygodni) Zamawiający przyjmie, że Wykonawca wpisał maksymalny termin realizacji (8 tygodni od daty podpisania umowy na realizację zamówienia) i przyzna Wykonawcy w tym kryterium 0 (zero) pkt.

2. Za najkorzystniejszą ofertę zostanie uznana oferta, która uzyska najwyższą liczbę punktów (P), gdzie P oznacza sumę uzyskanych punktów w kryteriach:

cena brutto (C) oraz termin realizacji zamówienia (T), zgodnie ze wzorem:

P = C + T

3. W sytuacji gdy cena najkorzystniejszej oferty będzie znacząco przewyższała środki zabezpieczone przez Zamawiającego w budżecie, Zamawiający zastrzega sobie możliwość przeprowadzenia dodatkowych negocjacji z Wykonawcą który złoży najkorzystniejszą ofertę.
4. W przypadku gdy wybrany Wykonawca odstąpi od podpisania umowy z Zamawiającym, możliwe jest podpisanie przez Zamawiającego umowy z kolejnym Wykonawcą, który w postępowaniu uzyskał kolejną najwyższą liczbę punktów.
5. Zamawiający może w toku badania i oceny ofert żądać od Oferentów dodatkowych wyjaśnień dotyczących treści złożonych ofert.
6. Zamawiający wyjaśni i poprawi w formularzu ofertowym:
   - oczywiste omyłki pisarskie,
   - oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
   - inne omyłki polegające na niezgodności oferty z opisem zawartym w zapytaniu ofertowym niepowodujące istotnych zmian w treści oferty.
7. Poprawienie przez Zamawiającego oczywistych omyłek pisarskich oraz rachunkowych i konsekwencji rachunkowych dokonanych poprawek nie wymaga uzyskania zgody wykonawcy. Wykonawca może nie wyrazić zgody na poprawienie przez zamawiającego innych omyłek polegających na niezgodności oferty z opisem zawartym w zapytaniu ofertowym niepowodujące istotnych zmian w treści oferty. Brak zgody Wykonawca musi wnieść na piśmie w wyznaczonym przez Zamawiającego terminie.
8. Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez dokonania wyboru żadnej z ofert, bez podania przyczyny, na każdym etapie prowadzonego postępowania. Z tytułu unieważnienia postępowania, Wykonawcy nie przysługuje żadne roszczenie wobec Zamawiającego.

Fundusze Europejskie na Rozwój Cyfrowy

13. Kontakt z Zamawiającym

1. Komunikacja w postępowaniu o udzielenie zamówienia, w tym składanie ofert, wymiana informacji między Zamawiającym a Wykonawcą oraz przekazywanie dokumentów i oświadczeń odbywa się pisemnie za pomocą portalu Bazy Konkurencyjności
2. Po stronie Zamawiającego osobą do kontaktów w sprawie zamówienia jest:

   Aneta Mazurczak
   Kierownik Wydziału Inwestycji i Zamówień Publicznych
   tel.: +48 95 748 89 57

   e-mail: wydzialinwestycji@powiatchoszczno.pl

3. W tytule wiadomości należy wskazać numer zapytania ofertowego – IZP.272.I.6.2024.
4. Każdy wykonawca ma prawo zwrócić się do zamawiającego o wyjaśnienie treści zapytania ofertowego. Pytania wykonawców muszą być przekazane za pośrednictwem portalu Baza Konkurencyjności.
5. Zamawiający udzieli odpowiedzi najpóźniej na 2 dni przed upływem terminu składania ofert pod warunkiem, że wniosek o wyjaśnienie treści zapytania ofertowego wpłynął do zamawiającego nie później niż 4 dni przed upływem terminu składania ofert.
6. Jeżeli zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w ust. 5, przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia oferty.
7. W przypadku, gdy wniosek o wyjaśnienie treści zapytania ofertowego nie wpłynął w terminie, o którym mowa w ust. 5, zamawiający nie ma obowiązku udzielania wyjaśnień oraz obowiązku przedłużania terminu składania ofert.

14. Wyjaśnienia oraz uzupełnienia do oferty

1. W toku badania ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonej oferty, treści oświadczeń, dokumentów,

pełnomocnictw i ich uzupełnienia

2. Jeżeli zaoferowana cena będzie rażąco niska w stosunku do przedmiotu zamówienia lub będzie budziła wątpliwości co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego lub wynikającymi z odrębnych przepisów, Zamawiający zwróci się do wykonawcy o udzielenie wyjaśnień, w tym złożenie dowodów dotyczących wyliczenia ceny. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu będzie spoczywać na Wykonawcy.
3. Zamawiający odrzuci ofertę Wykonawcy, który nie udzieli wyjaśnień, o których mowa powyżej lub jeżeli dokonana ocena tych wyjaśnień wraz ze złożonymi dowodami potwierdzi, że zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.

15. Klauzula informacyjna RODO

1. Klauzula informacyjna z art. 13 RODO Zgodnie z art. 13 ust.1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016 r., str. 1), dalej „RODO”, informuję, że:

   Administratorem danych osobowych Wykonawcy jest:

   Starosta Choszczeński

   ul. Nadbrzeżna 2

   73-200 Choszczno

   Inspektorem ochrony danych osobowych w Starostwie Powiatowym w Choszcznie jest:

   Pan Piotr Barwina

   Adres e-mail: iod.choszczno@barwina.eu

   Telefon: 693 417 982

2. Zamawiający przetwarza dane osobowe zebrane w niniejszym postępowaniu o udzielenie zamówienia publicznego w sposób gwarantujący zabezpieczenie przed ich bezprawnym rozpowszechnianiem.
3. Zamawiający udostępnia dane osobowe, o których mowa w art. 10 RODO w celu umożliwienia korzystania ze środków ochrony prawnej, o których mowa w dziale VI Pzp, do upływu terminu do ich wniesienia.
4. Do przetwarzania danych osobowych, o których mowa w art. 10 RODO mogą być dopuszczone wyłącznie osoby posiadające upoważnienie. Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w poufności.
5. Dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z prowadzeniem niniejszego postępowania o udzielenie zamówienia publicznego oraz jego rozstrzygnięciem, jak również, jeżeli nie ziszczą się przesłanki określone w art. 255-256 Pzp – w celu zawarcia umowy w sprawie zamówienia publicznego oraz jej realizacji, a także udokumentowania postępowania o udzielenie zamówienia i jego archiwizacji.
6. Odbiorcami danych osobowych będą osoby lub podmioty, którym dokumentacja postępowania zostanie udostępniona w oparciu o przepisy ustawy Pzp, a także na podstawie ustawy o dostępie do informacji publicznej.
7. Dane osobowe pozyskane w związku z prowadzeniem niniejszego postępowania o udzielenie zamówienia publicznego będą przechowywane, zgodnie z art. 78 ust. 1 Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia publicznego, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy w sprawie zamówienia publicznego.
8. Niezależnie od postanowień pkt 7 powyżej, w przypadku zawarcia umowy w sprawie zamówienia publicznego, dane osobowe będą przetwarzane do upływu okresu przedawnienia roszczeń wynikających z umowy w sprawie zamówienia publicznego.

9. Dane osobowe pozyskane w związku z prowadzeniem niniejszego postępowania o udzielenie zamówienia mogą zostać przekazane podmiotom świadczącym usługi doradcze, w tym usługi prawne i konsultingowe.
10. Stosownie do art. 22 RODO, decyzje dotyczące danych osobowych nie będą podejmowane w sposób zautomatyzowany.
11. Osoba, której dotyczą pozyskane w związku z prowadzeniem niniejszego postępowania dane osobowe, ma prawo:
    1) do dostępu do swoich danych osobowych – zgodnie z art. 15 RODO, przy czym w sytuacji, gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1 – 3 RODO wymagałoby niewspółmiernie dużego wysiłku Zamawiający może żądać wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty bieżącego bądź zakończonego postępowania o udzielenie zamówienia publicznego;
    2) do sprostowania swoich danych osobowych – zgodnie z art. 16 RODO, przy czym skorzystanie z uprawnienia do sprostowania lub uzupełnienia danych osobowych, o którym mowa w art. 16 RODO, nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego, ani zmianą postanowień umowy w zakresie niezgodnym z Pzp oraz nie może naruszać integralności protokołu oraz jego załączników;
    3) do żądania od Zamawiającego – jako administratora, ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO, przy czym prawo do ograniczenia przetwarzania danych nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego; prawo to nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego;

4) do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych w przypadku uznania, iż przetwarzanie jej danych osobowych narusza przepisy o ochronie danych osobowych, w tym przepisy RODO.

12. Obowiązek podania danych osobowych jest wymogiem ustawowym określonym w przepisach Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych określa Pzp.
13. Osobie, której dane osobowe zostały pozyskane przez Zamawiającego w związku z prowadzeniem niniejszego postępowania o udzielenie zamówienia publicznego nie przysługuje:
    1) prawo do usunięcia danych osobowych, o czym przesądza art. 17 ust. 3 lit. b, d lub e RODO,
    2) prawo do przenoszenia danych osobowych, o którym mowa w art.. 20 RODO, określone w art. 21 RODO prawo sprzeciwu wobec przetwarzania danych osobowych, a to z uwagi na fakt, że podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. c RODO.
14. Dane osobowe mogą być przekazywane do organów publicznych i urzędów państwowych lub innych podmiotów upoważnionych na podstawie przepisów prawa lub wykonujących zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej, w szczególności do podmiotów prowadzących działalność kontrolną wobec Zamawiającego. Dane osobowe są przekazywane do podmiotów przetwarzających dane w imieniu administratora danych osobowych.
15. Pozostałe informacje dotyczące obowiązku informacyjnego RODO, zostały zamieszczone na stronie internetowej Zamawiającego, dostępne pod poniżej wskazanym adresem: http://www.powiatchoszczno.pl/wazne/klauzula-informacyjna-rodo/

Załączniki:

1. Formularz oferty.
2. Wykaz usług.

3. Wykaz osób przeznaczonych do realizacji zamówienia.
4. Projektowane postanowienia umowy.