

Załącznik nr 1 do zaproszenia do szacowania

Znak sprawy: BDG-WI.....2026

OPIS PRZEDMIOTU ZAMÓWIENIA

(opis przedmiotu szacowania)

Dodatkowe wsparcie dla posiadanych urządzeń NGFW w GDOŚ na okres 12 miesięcy – konsultacje, zarządzanie, nowe funkcjonalności**I. WPROWADZENIE**

1. Przedmiotem zamówienia jest usługa obejmująca przegląd konfiguracji i wykonanie prac koniecznych na czterech eksploatowanych przez Zamawiającego urządzeniach klasy Next Generation Firewall (NGFW) Stormshield (aktualizacja oprogramowania, utwardzenie, uporządkowanie polityki bezpieczeństwa, weryfikacja wysokiej dostępności, kopie zapasowe, dokumentacja), a następnie świadczenie usługi wsparcia w formie puli roboczogodzin przez okres 12 miesięcy – w zakresie konsultacji, bieżącego zarządzania konfiguracją i uruchamiania nowych funkcjonalności.
2. Celem zamówienia jest utrzymanie urządzeń NGFW jako technicznego środka zarządzania ryzykiem: zapewnienie wspieranej i aktualnej wersji oprogramowania, ograniczenie powierzchni ataku na zaporę i strefę DMZ, rozliczalność działań administracyjnych, ciągłość działania styku z siecią Internet oraz możliwość bezpiecznego wprowadzania zmian i nowych funkcji w okresie 12 miesięcy.
3. Zamówienie jest finansowane w ramach Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności (dalej: „KPO”), Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo - Cyberbezpieczny Rząd, w zakresie wydatków kwalifikowalnych poniesionych do dnia 31 grudnia 2026 r., a w pozostałym zakresie – ze środków budżetowych Zamawiającego.
4. Zamawiający: Skarb Państwa – Generalna Dyrekcja Ochrony Środowiska, Al. Jerozolimskie 136, 02-305 Warszawa, NIP 7010151052, REGON 141628410.
5. Użyte w OPZ określenia oznaczają:
 - 1) **Urządzenia** – urządzenia NGFW Stormshield eksploatowane przez Zamawiającego w siedzibie przy Al. Jerozolimskich 136 w Warszawie, wymienione w rozdz. II ust. 1;
 - 2) **SNS** – system operacyjny Urządzeń (Stormshield Network Security) wraz z narzędziami administracyjnymi producenta;
 - 3) **HA** – konfiguracja wysokiej dostępności w trybie active-passive (klaster dwóch Urządzeń: aktywne i zapasowe);
 - 4) **Okno serwisowe** – uzgodniony z Zamawiającym przedział czasu, w którym dopuszczalne są prace mogące spowodować przerwę lub zakłócenie ruchu sieciowego;
 - 5) **Etap I, Etap II** – odpowiednio: przegląd i prace konieczne (rozdz. III) oraz usługa wsparcia (rozdz. IV);
 - 6) **rbh** – roboczogodzina, tj. 60 minut pracy jednego specjalisty Wykonawcy;
 - 7) **Awaria** – stan, w którym Urządzenia lub klaster HA nie przekazują ruchu sieciowego, nie realizują polityki bezpieczeństwa, nie zestawiają tuneli VPN albo utracono możliwość zarządzania nimi;
 - 8) **dzień roboczy** – dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy; godziny robocze: 8:00–16:00.

II. STAN OBECNY I ZAKRES ZAMÓWIENIA

1. Zamawiający eksploatuje następujące Urządzenia:

Lp.	Model	Liczba	Funkcja
1	Stormshield SN1100	2 szt.	zapora brzegowa sieci GDOŚ (styk z Internetem, sieć wewnętrzna); klaster HA active-passive
2	Stormshield SN520	2 szt.	zapora strefy DMZ (usługi publikowane); klaster HA active-passive

- Urządzenia posiadają aktywną subskrypcję producenta (aktualizacje oprogramowania i wsparcie producenta), utrzymywaną przez Zamawiającego. Szczegółowe dane (numery seryjne, wersje SNS, konfiguracja klastrów HA, zakres licencji i modułów ochrony, schemat sieci) zostaną przekazane Wykonawcy po zawarciu umowy, z zachowaniem zasad poufności.
- Zamówienie nie obejmuje: dostawy sprzętu, licencji ani subskrypcji producenta (Zamawiający zapewnia ich ważność we własnym zakresie); naprawy sprzętowej Urządzeń w ramach gwarancji producenta; integracji Urządzeń z systemami usługi SOC świadczonej na rzecz Zamawiającego na podstawie odrębnej umowy; monitorowania ruchu w trybie 24/7 i obsługi incydentów w imieniu Zamawiającego; czynności objętych usługą wsparcia powdrożeniowego dla urządzeń NGFW dostarczonych na podstawie odrębnych umów Zamawiającego. Szkolenie nie jest przedmiotem zamówienia; instruktaż techniczny, o którym mowa w rozdz. III ust. 14, stanowi element odbioru Etapu I.
- Zamawiający zapewni: zdalny dostęp przez VPN wskazany przez Zamawiającego, imienne konta z uprawnieniami niezbędnymi do realizacji prac, dostęp do siedziby w uzgodnionych terminach (jeżeli prace wymagają obecności), zasób sieciowy na kopie zapasowe konfiguracji, konfigurację po stronie Microsoft 365 niezbędną do wysyłki powiadomień e-mail oraz koordynację z wykonawcą usługi SOC.

III. ETAP I – PRZEGLĄD I PRACE KONIECZNE

- Termin: 30 dni od dnia zawarcia umowy, nie później niż do dnia 15 grudnia 2026 r.
- Przegląd i Raport z przeglądu.** W terminie 7 dni od dnia zawarcia umowy Wykonawca przekaże do akceptacji Raport z przeglądu zawierający co najmniej:
 - inwentaryzację: modele i numery seryjne, wersje SNS, stan licencji, subskrypcji i modułów ochrony, stan klastrów HA, interfejsy i VLAN, routing, NAT, tunele VPN, obiekty, konta administracyjne i metody uwierzytelniania, uruchomione usługi, konfigurację logowania i kopii zapasowych;
 - analizę polityki filtrowania i NAT z wykorzystaniem liczników trafień: reguły nieużywane, zdublowane, przesłonięte i nadmiernie szerokie (np. „any-any”);
 - ocenę zgodności konfiguracji z zaleceniami producenta dotyczącymi utwardzania oraz uznanymi dobrymi praktykami (np. CIS, ANSSI lub równoważnymi), z listą niezgodności i oceną ryzyka (wysokie/średnie/niskie);
 - docelową wersję SNS (wspieraną przez producenta, rekomendowaną do zastosowań produkcyjnych, np. gałąź o wydłużonym wsparciu) i plan aktualizacji z planem wycofania zmian;
 - plan prac koniecznych z harmonogramem, oknami serwisowymi i oceną wpływu na dostępność usług;
 - rekomendacje nowych funkcjonalności możliwych do uruchomienia w ramach posiadanych licencji, do rozważenia w Etapie II.

3. Zamawiający w terminie 3 dni roboczych zaakceptuje Raport z przeglądu albo zgłosi uwagi. Prace, o których mowa w ust. 4–11, Wykonawca wykonuje zgodnie z zaakceptowanym Raportem, a zmiany polityki filtrowania – wyłącznie po akceptacji listy zmian przez Zamawiającego.
4. **Kopia zapasowa przed zmianami.** Przed rozpoczęciem prac – pełna, zaszyfrowana kopia konfiguracji każdego Urządzenia, przekazana Zamawiającemu i umożliwiająca przywrócenie stanu sprzed zmian.
5. **Aktualizacja SNS** do wersji wskazanej w zaakceptowanym Raporcie, w Oknie serwisowym, z zachowaniem kolejności właściwej dla klastrów HA tak, aby ograniczyć przerwę w przekazywaniu ruchu; weryfikacja działania po aktualizacji (ruch, reguły, VPN, logowanie).
6. **Utwardzenie dostępu administracyjnego:**
 - 1) wyłącznie imienne konta administratorów, uwierzytelnianie kontami domenowymi (LDAPS / Active Directory) – o ile wspierane – z przypisaniem ról i uprawnień;
 - 2) uwierzytelnianie wieloskładnikowe dostępu administracyjnego, z wykorzystaniem mechanizmów dostępnych w SNS lub w infrastrukturze Zamawiającego;
 - 3) ograniczenie dostępu do interfejsów administracyjnych do wskazanych sieci i stacji administratorów; wyłącznie protokoły szyfrowane (HTTPS z TLS 1.2 lub 1.3, SSH), poprawne certyfikaty;
 - 4) wyłączenie nieużywanych usług i protokołów, SNMP w wersji 3 (jeżeli używane), limit czasu bezczynności sesji, polityka haseł, synchronizacja czasu (NTP), rejestrowanie działań administracyjnych;
 - 5) wdrożenie podziału ról administracyjnych (RBAC), w tym dedykowanego profilu o uprawnieniach wyłącznie do odczytu (Read-Only) na potrzeby audytu i monitoringu SOC.
7. **Polityka filtrowania i NAT:** usunięcie lub wyłączenie reguł nieużywanych, zdublowanych i przesłoniętych, zawężenie reguł nadmiernie szerokich, uporządkowanie kolejności, usunięcie lub dezaktywacja nieużywanych obiektów sieciowych (hosty, grupy, usługi), opisy (komentarze) reguł i obiektów, konfiguracja blokowania geolokalizacyjnego (GeoIP) na zaporze brzegowej dla krajów wysokiego ryzyka, reguła domyślnie blokująca z rejestrowaniem – w zakresie zaakceptowanym przez Zamawiającego. W zakresie ruchu do usług Microsoft 365 (m.in. Exchange Online, SharePoint Online/OneDrive, Teams, Microsoft Entra ID) Wykonawca:
 - 1) zdefiniuje obiekty i reguły oparte na publikowanych przez Microsoft wykazach adresów IP i nazw FQDN (kategorie Optimize, Allow, Default), z mechanizmem ich automatycznej lub okresowej aktualizacji, opisanym w dokumentacji;
 - 2) wyłączy z inspekcji SSL/TLS i filtrowania treści ruch z kategorii Optimize, zgodnie z zaleceniami Microsoft, z zachowaniem rejestrowania połączeń;
 - 3) zapewni poprawne działanie uwierzytelniania (Entra ID, MFA) oraz komunikacji audio-wideo Teams (w tym ruch UDP), bez nadmiernie szerokich reguł;
 - 4) skonfiguruje reguły dla wysyłki poczty przez Exchange Online (konektor lub przekaźnik SMTP) ograniczone do hostów wskazanych przez Zamawiającego (m.in. serwery wysyłające powiadomienia, urządzenia wielofunkcyjne).
8. **Strefa DMZ (SN520):** weryfikacja segmentacji DMZ–sieć wewnętrzna–Internet według zasady najmniejszych uprawnień, przegląd publikacji usług i reguł translacji, włączenie ochrony IPS dla usług publikowanych.
9. **Mechanizmy ochrony i VPN:** weryfikacja i strojenie profili ochrony (zapobieganie włamaniom, ochrona antywirusowa, filtrowanie URL, reputacja adresów) w zakresie

posiadanych licencji; przegląd tuneli VPN (IPsec i dostęp zdalny) pod kątem aktualnych algorytmów kryptograficznych (m.in. IKEv2, PFS, wycofanie algorytmów przestarzałych).

10. **Wysoka dostępność (active-passive):** weryfikacja synchronizacji konfiguracji i stanu sesji w obu klastrach HA, parametrów wykrywania awarii (monitorowane interfejsy, łącza HA, priorytety), test przełączenia na Urządzenie zapasowe i powrotu w Oknie serwisowym, z pomiarem czasu przełączenia.
11. **Logowanie, powiadomienia i kopie zapasowe:**
 - 1) weryfikacja przekazywania dzienników zdarzeń (syslog, w miarę możliwości szyfrowany) do odbiorców wskazanych przez Zamawiającego; zmiany dotyczące przekazywania dzienników do usługi SOC – wyłącznie w uzgodnieniu z Zamawiającym i wykonawcą usługi SOC, bez przejmowania jego zadań;
 - 2) powiadomienia e-mail o zdarzeniach krytycznych (m.in. Awaria, przełączenie HA, zmiana konfiguracji, alarmy wysokiego poziomu) przez pocztę Zamawiającego w usłudze Microsoft 365, metodą wspieraną przez Microsoft i zabezpieczoną TLS;
 - 3) automatyczne, cykliczne i szyfrowane kopie konfiguracji wszystkich Urządzeń na zasób Zamawiającego oraz przetestowana procedura odtworzenia konfiguracji.
12. **Testy akceptacyjne** z udziałem Zamawiającego, co najmniej: wersja SNS zgodna z Raportem na wszystkich Urządzeniach; poprawne przekazywanie ruchu i działanie usług publikowanych w DMZ; zestawianie tuneli VPN; przełączenie HA bez utraty łączności ponad czas uzgodniony w Raporcie; logowanie administratora z MFA i blokada dostępu spoza dozwolonych sieci; działanie profilu Read-Only (brak możliwości zmian); działanie blokady GeoIP; poprawne działanie usług Microsoft 365 (poczta, OneDrive/SharePoint, Teams z audio-wideo, logowanie z MFA) i wysyłki SMTP ze wskazanych hostów; odbiór powiadomienia e-mail; przekazywanie dzienników do wskazanych odbiorców; wykonanie i odtworzenie kopii konfiguracji.
13. **Dokumentacja powykonawcza** w języku polskim (format edytowalny i PDF): Raport z przeglądu z informacją o usuniętych niezgodnościach; schemat logiczny sieci w zakresie Urządzeń; opis konfiguracji; macierz reguł filtrowania i NAT z opisami (w tym reguł dla Microsoft 365 i sposobu aktualizacji obiektów); wykaz tuneli VPN i parametrów kryptograficznych; rejestr zmian wykonanych w Etapie I; procedury eksploatacyjne (aktualizacja SNS, przełączenie i przywrócenie HA, odtworzenie konfiguracji z kopii, procedura wymiany awaryjnej urządzenia w ramach RMA producenta (Disaster Recovery), zarządzanie kontami administratorów, dodawanie reguł i obiektów). Pliki konfiguracji przekazuje się w postaci zaszyfrowanej.
14. Wykonawca w ramach odbioru Etapu I przeprowadzi instruktaż techniczny (w wymiarze do 4 godzin, stacjonarnie lub zdalnie) dla administratorów Zamawiającego, prezentujący wprowadzone zmiany, nowe funkcje zaktualizowanego systemu SNS oraz procedury eksploatacyjne.
15. Odbiór Etapu I następuje protokołem odbioru po pozytywnych testach akceptacyjnych, przekazaniu dokumentacji powykonawczej i przeprowadzeniu instruktażu technicznego.

IV. ETAP II – USŁUGA WSPARCIA (PULA ROBOCZOGODZIN)

1. Pula do 60 rbh do wykorzystania przez 12 miesięcy od dnia odbioru Etapu I bez uwag. Zamawiający nie jest zobowiązany do wykorzystania puli w całości ani w części; wynagrodzenie przysługuje wyłącznie za rbh faktycznie wykorzystane, a Wykonawcy nie przysługują roszczenia z tytułu niewykorzystania puli.
2. Pula może być wykorzystana w szczególności na:

- 1) **konsultacje** – doradztwo w zakresie architektury i segmentacji sieci, polityki bezpieczeństwa, planowanych zmian, analizy zdarzeń i alertów z Urzędzeń, wsparcie przy audytach i kontrolach;
 - 2) **zarządzanie** – zmiany reguł filtrowania, NAT, obiektów, routingu i tuneli VPN, dostosowanie reguł do zmian usług Microsoft 365, aktualizacje SNS wydane w okresie 12 miesięcy, okresowe przeglądy konfiguracji, diagnoza problemów niebędących wadą objętą gwarancją, przywracanie konfiguracji;
 - 3) **nowe funkcjonalności** – uruchamianie i konfiguracja funkcji dostępnych w ramach posiadanych licencji (np. rozszerzenie ochrony IPS, filtrowanie URL, identyfikacja użytkowników, polityki dostępu zdalnego z MFA, nowe strefy i segmenty sieci, publikacja nowych usług w DMZ).
3. Zasady zgłaszania potrzeb i poziom usług (SLA):
- 1) **Zgłoszenie** – przekazują osoby wskazane przez Zamawiającego, przez uzgodniony kanał (adres e-mail lub system zgłoszeń Wykonawcy), w dni robocze w godz. 8:00–16:00; zgłoszenie przekazane po godz. 16:00 lub w dniu wolnym uważa się za przekazane o godz. 8:00 następnego dnia roboczego. Zgłoszenie zawiera opis potrzeby lub problemu, oczekiwany rezultat oraz wskazanie, czy dotyczy Awarii;
 - 2) **Reakcja** – do 4 godzin roboczych od zgłoszenia: potwierdzenie przyjęcia z nadaniem numeru, wstępna diagnoza oraz propozycja zakresu prac, terminu wykonania i szacowanej liczby rbh. W przypadku Awarii Wykonawca w tym czasie rozpoczyna prace naprawcze, a zakres i liczbę rbh przedstawia niezwłocznie;
 - 3) **Przyjęcie do realizacji** – Zamawiający akceptuje propozycję wiadomością e-mail, zgłasza uwagi albo rezygnuje ze zgłoszenia. Czas przyjęcia, diagnozy i wyceny zgłoszenia nie podlega rozliczeniu w rbh, a zgłoszenie niezaakceptowane nie jest rozliczane;
 - 4) **Realizacja** – do 2 dni roboczych od przyjęcia zgłoszenia do realizacji. Dłuższy termin jest dopuszczalny wyłącznie dla zadań rozwojowych (nowe funkcjonalności), których pracochłonność obiektywnie to uzasadnia, jeżeli Wykonawca wskaże go w propozycji i Zamawiający go zaakceptuje. Zmiany wymagające przerwy w ruchu realizowane są w Oknie serwisowym;
 - 5) **Zamknięcie** – Wykonawca informuje o wykonaniu, opisuje wykonane czynności, faktyczną liczbę rbh i – jeżeli dotyczy – aktualizuje dokumentację powykonawczą i rejestr zmian; Zamawiający potwierdza wykonanie albo zgłasza zastrzeżenia w ciągu 2 dni roboczych. Przekroczenie zaakceptowanej liczby rbh wymaga uprzedniej zgody Zamawiającego;
 - 6) **Rejestr i rozliczenie** – każde zgłoszenie jest rejestrowane (numer, data i godzina zgłoszenia, reakcji, przyjęcia do realizacji i zakończenia, opis, wykonane czynności, liczba rbh). Rozliczenie następuje miesięcznie, w jednostkach 0,5 rbh, wyłącznie za zgłoszenia zamknięte w danym miesiącu, na podstawie protokołu realizacji zgłoszeń zatwierdzonego przez Zamawiającego; protokół stanowi podstawę wystawienia faktury.
4. Każda zmiana konfiguracji w Etapie II jest poprzedzona wykonaniem kopii konfiguracji i obejmuje plan wycofania zmian. Wykonawca prowadzi rejestr w sposób umożliwiający Zamawiającemu weryfikację dotrzymania czasów reakcji i realizacji; przekroczenia wykazuje w protokole realizacji zgłoszeń.

V. GWARANCJA

1. Wykonawca udziela 12-miesięcznej gwarancji, liczonej od dnia odbioru Etapu I, na prawidłowe działanie konfiguracji wykonanej w Etapie I, w tym mechanizmów HA, powiadomień i kopii zapasowych.
2. Usuwanie wad objętych gwarancją jest nieodpłatne i nie pomniejsza puli rbh. Do zgłaszania wad stosuje się zasady i czasy reakcji oraz realizacji określone w rozdz. IV ust. 3, z tym że czas usuwania wady nie jest rozliczany w rbh. Gwarancja nie obejmuje wad sprzętowych Urządzeń ani błędów oprogramowania producenta – w tym zakresie Wykonawca wspiera Zamawiającego w kontakcie z producentem w ramach puli rbh.

VI. WYMAGANIA OGÓLNE

1. Prace wykonywane są z zachowaniem ciągłości działania infrastruktury Zamawiającego; czynności mogące spowodować przerwę Wykonawca uzgadnia z wyprzedzeniem co najmniej 2 dni roboczych (z wyjątkiem usuwania Awarii) i wykonuje w Oknie serwisowym.
2. Wykonawca stosuje się do polityk bezpieczeństwa Zamawiającego, korzysta wyłącznie z przydzielonych kont imiennych, nie kopiuje konfiguracji i danych poza infrastrukturę Zamawiającego (z wyjątkiem uzgodnionej diagnostyki u producenta, po anonimizacji), a dokumentację przekazuje w zaszyfrowanych archiwach (AES-256), z hasłem przekazanym innym kanałem.
3. Członkowie zespołu Wykonawcy składają oświadczenie o zachowaniu poufności przez okres obowiązywania umowy oraz 5 lat po jej wygaśnięciu.
4. Dzienniki zdarzeń Urządzeń zawierają dane osobowe (m.in. adresy IP, identyfikatory użytkowników); Wykonawca zawrze z Zamawiającym umowę powierzenia przetwarzania danych osobowych (art. 28 RODO).
5. Wykonawca nie dostarcza oprogramowania wymagającego zakupu licencji przez Zamawiającego; narzędzia pomocnicze wykorzystywane przez Wykonawcę nie mogą pozostawać w środowisku Zamawiającego bez jego zgody.
6. Oznakowanie KPO: wszystkie dokumenty wytworzone w ramach zamówienia (Raport z przeglądu, dokumentacja, raporty, protokoły) Wykonawca oznacza zgodnie z Księgą Identyfikacji Wizualnej KPO oraz Strategią promocji i informacji KPO (<https://www.kpo.gov.pl/strony/o-kpo/dla-instytucji/dokumenty/strategia-promocji-i-informacji-kpo/>).
7. Klauzula ICT: Wykonawca oferuje wyłącznie produkty, usługi i procesy ICT, które na dzień składania ofert nie są objęte rekomendacją, o której mowa w art. 33 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa, ani decyzją o uznaniu dostawcy za dostawcę wysokiego ryzyka (art. 67b ust. 15 tej ustawy); dotyczy to także narzędzi zdalnego dostępu i systemu zgłoszeń Wykonawcy.
8. Zasada DNSH: przedmiot zamówienia nie wyrządza znaczącej szkody celom środowiskowym; usługa przedłuża bezpieczną eksploatację posiadanych Urządzeń bez zakupu nowego sprzętu, prace wykonywane są co do zasady zdalnie, a dokumenty przekazywane wyłącznie w formie elektronicznej.
9. Zakaz podwójnego finansowania: zakres zamówienia nie pokrywa się z usługami realizowanymi na podstawie innych umów Zamawiającego (w tym umowy na usługę SOC oraz umów obejmujących wsparcie powdrożeniowe urządzeń NGFW); Wykonawca opisuje czynności w protokołach w sposób umożliwiający ich jednoznaczne przypisanie do niniejszego zamówienia i do Urządzeń.
10. Komunikacja i dokumentacja – w języku polskim.

VII. PLANOWANE WARUNKI UDZIAŁU I KRYTERIA OCENY OFERT

Informacja ma charakter orientacyjny i służy oszacowaniu kosztów; ostateczne warunki i kryteria zostaną określone w zapytaniu ofertowym.

1. Warunek udziału – personel: co najmniej 1 inżynier posiadający ważny certyfikat producenta potwierdzający kompetencje w zakresie administrowania urządzeniami Stormshield Network Security (np. CSNA lub wyższy) albo certyfikat równoważny, który w okresie ostatnich 3 lat uczestniczył w co najmniej 1 usłudze wdrożenia lub utrzymania urządzeń Stormshield.
2. Planowane kryteria oceny ofert:

Kryterium	Opis	Waga
Cena łączna	cena brutto za Etap I oraz 60 rbh Etapu II; $P_c = (C_{min} / C_{bad}) \times 60$	60 pkt
Cena 1 rbh	cena brutto za 1 rbh w Etapie II; $P_r = (R_{min} / R_{bad}) \times 10$	10 pkt
Doświadczenie inżyniera	udział inżyniera skierowanego do realizacji zamówienia w więcej niż 3 usługach wdrożenia lub utrzymania urządzeń Stormshield w konfiguracji HA, w jednostkach zatrudniających powyżej 100 użytkowników, w okresie ostatnich 3 lat: więcej niż 3 usługi – 30 pkt; 3 lub mniej – 0 pkt	30 pkt