

**Załącznik Nr 3 do SWZ – formularz oferty**

**Formularz oferty z załącznikami**

wersja edytowalna - plik:

„5. Formularz oferty z załącznikami (zał. nr 3-8 do SWZ).doc



**Załącznik Nr 3 do SWZ - Formularz oferty**

 ......................................................

 (miejscowość i data )

|  |  |
| --- | --- |
| .......................................................... Nazwa Wykonawcy  | Adres ....................................................................... **E-mail** ...................................................................... |
| NIP |  |
| .......................................................... Nazwa Wykonawcy  | Adres ....................................................................... **E-mail** ...................................................................... |
| NIP |  |

|  |  |
| --- | --- |
|  **Pełnomocnik**(dotyczy Wykonawców wspólnie ubiegających się o zamówienia) |  |

# OFERTA

# w trybie podstawowym bez negocjacji

 Zamawiający : **Gmina Nysa**

 **Urząd Miejski w Nysie**

ul. Kolejowa 15, 48-300 Nysa

W odpowiedzi na ogłoszenie o zamówieniu w **trybie podstawowym bez negocjacji,** oferujemy wykonanie zamówienia pn.:

**Wymiana systemu zapór sieciowych w Urzędzie Miejskim w Nysie,**

*w ramach realizacji projektu Cyberbezpieczny Samorząd - Gmina Nysa (umowa o powierzenie grantu: FERC.02.02-CS.01-001/23/0675/ FERC.02.02-CS.01-001/23/2024 z 04.06.2024 r.)*

poprzez wymianę urządzeń zabezpieczeń ruchu sieciowego czyli dostawę i wdrożenie dwóch nowych urządzeń typu Next Generation Firewall z licencjami, oraz z serwisem gwarancyjnym - zgodnie z poniższą specyfikacją:

1. **System zapór sieciowych**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu (element****/cecha)** | **Opis wymaganych minimalnych parametrów technicznych** | ***Opis rozwiązania będącego przedmiotem oferty*** | ***Part Number (numer części)*** | ***Jedn. miary*** | ***Ilość*** |
|  | Obudowa | Urządzenie musi być przeznaczone do montażu w szafie Rack 19” i jego wysokość nie może przekroczyć 1U. Urządzenie musi być dostarczone z wszystkimi niezbędnymi elementami umożliwiającymi montaż urządzenia w szafie. |  |  | **Szt.** | **2** |
|  | Porty | Urządzenie musi posiadać:1. co najmniej 12 portów 1-Gigabit Ethernet RJ45,
2. co najmniej 6 portów 1 Gigabit Ethernet SFP oraz co najmniej 4 porty 10 Gigabit Ethernet SFP+ obsługujące moduły optyczne SR oraz LR,
3. co najmniej 1 port 1-Gigabit Ethernet RJ45 wyłącznie do celów zarządzania,
4. co najmniej 1 port konsolowy,

co najmniej 1 port (10GE lub szybszy) i port 1-Gigabit Ethernet RJ45 dla celów połączenia urządzeń w klaster (high availability) lub dwa porty 1-Gigabit Ethernet RJ45. Porty te muszą być traktowane jako dodatkowe względem wymaganych przez Zamawiającego. Nie dopuszcza się wykorzystania do celu klastrowania portów opisanych w podstawowych wymaganiach. |  |  |
|  | Pamięć | Urządzenie musi posiadać co najmniej 120 GB pojemności dyskowej na przechowywanie logów i firmware. |  |  |
|  | Zasilanie | Urządzenie musi posiadać co najmniej dwa redundantne zasilacze. Zamawiający nie dopuszcza stosowania zewnętrznych zasilaczy do spełnienia tego warunku. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia. |  |  |
|  | Wydajność urządzenia | Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:1. 8 Gbps dla rozpoznawania i kontroli aplikacji - przy transakcjach 64KB,
2. 4 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: włączone wszystkie sygnatury IPS, antywirus, antyspyware, blokowanie typów plików, z włączonym logowaniem na dyski urządzenia - przy transakcjach 64KB,
3. 4 Gbps dla IPSec VPN - przy transakcjach 64KB,
4. 90 000 nowych połączeń na sekundę,

900 000 jednoczesnych sesji. |  |  |
|  | Wirtualizacja | Urządzenie musi obsługiwać nie mniej niż 6 wirtualnych routerów, posiadających odrębne tablice routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu, w pojedynczej wirtualnej instancji firewall. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie niż wskazana w pozostałych wymaganiach dla urządzenia.Urządzenie musi posiadać możliwość licencyjnego ustanowienia co najmniej 6 wirtualnych instancji firewall (określanych jako kontekst/domena/system). Każda z instancji musi pozwalać na konfigurację niezależnych oraz odrębnych od innych instancji - polityk bezpieczeństwa (co najmniej dla IPS, AV i współpracy z sandboxem), tablicy routingu oraz realizacji zdalnego dostępu. |  |  |
|  | Funkcjonalności | Urządzenie musi posiadać możliwość zdefiniowania co najmniej 50 stref bezpieczeństwa.Urządzenie musi posiadać architekturę z odseparowanymi zasobami. Procesory zarządzające oraz pamięć (Management Plane) muszą być oddzielne od procesorów i pamięci przetwarzających ruch sieciowy (Data Plane).Urządzenie musi posiadać wydzielony moduł do zarządzania, tak aby nadmierne obciążenie ruchem sieciowym (Data Plane) urządzenia nie blokowało funkcjonowania części zarządzającej (Management Plane). Nie może powodować problemów z konfigurowaniem czy monitorowaniem urządzenia, dostępem do interfejsu GUI i CLI.Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 9900 reguł polityki bezpieczeństwa oraz 2900 reguł NAT.Urządzenie musi działać w następujących trybach pracy:1. routera (tzn. w warstwie 3 modelu OSI),
2. mostu (tzn. w warstwie 2 modelu OSI),
3. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; musi pracować w trybie przezroczystego łączenia interfejsów w pary),
4. w trybie pasywnego nasłuchu (sniffer/tap).

Urządzenie musi umożliwiać pracę we wszystkich wymienionych powyżej trybach, jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.Urządzenie musi posiadać separację logiczną zasobów służących do przetwarzania ruchu, od zasobów służących do zarządzania urządzeniem.Urządzenie musi posiadać dedykowane zasoby/rdzenie procesora/procesorów do funkcji zarządzania urządzeniem lub możliwość ustawienia dedykowanych zasobów/rdzeni procesora/procesorów do funkcji zarządzania urządzeniem.Urządzenie musi wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Podinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać min. 4000 znaczników VLAN.Urządzenie musi wspierać protokół LACP.Urządzenie musi zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).Urządzenie musi działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.Urządzenie musi uwzględniać polityki zabezpieczeń:1. adresy IP źródłowe i docelowe,
2. protokoły i usługi sieciowe,
3. aplikacje,
4. kategorie URL,
5. użytkowników aplikacji i grupy,
6. reakcje zabezpieczeń,
7. logowanie zdarzeń (początek i koniec sesji),
8. strefa wejściowa i wyjściowa.

Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65535 dostępnych portach. Przy tym wydajność kontroli firewalla stanowego i kontroli aplikacji całego ruchu nie może być mniejsza, niż wskazano w wymaganiach wydajnościowych urządzeń.Urządzenie musi wykrywać co najmniej 4000 predefiniowanych aplikacji wspieranych przez producenta (takich jak: DNS over HTTPS, Telegram, Skype, Tor, BitTorrent, MQTT, Modbus, DNP3, Siemens S7) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.Urządzenie musi obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.Urządzenie musi obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.Urządzenie musi posiadać osobny zestaw reguł definiujący politykę translacji adresów NAT rozdzielny od polityk innych typów.Urządzenie musi posiadać osobny zestaw reguł definiujący politykę kształtowania ruchu (QoS) rozdzielny od polityk innych typów.Urządzenie musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. routing-based VPN).Dla fazy 1 i 2 tunelu site-to-site urządzenie musi posiadać wsparcie dla algorytmów szyfrowania minimum AES-256-CBC, AES-256-GCM, HMAC-SHA- 384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.Urządzenie musi posiadać osobny zestaw reguł definiujący politykę deszyfracji rozdzielny od polityk innych typów.Urządzenie musi posiadać osobny zestaw reguł definiujący politykę uwierzytelniania rozdzielny od polityk innych typów.W urządzeniu musi być odnotowywane wykonywanie operacji translacji adresów NAT w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami NAT.Urządzenie musi pozwalać na selektywne wysyłanie logów na zasoby zewnętrzne w zależności od ich rodzaju.Urządzenie musi zapewniać możliwość odszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.3.Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa.Urządzenie musi posiadać możliwość odnotowywania wykonywania operacji odszyfrowania ruchu w logach urządzenia w dedykowanej do tego celu sekcji. Logi muszą zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.Urządzenie musi umożliwiać wykorzystanie mechanizmów filtrowania URL przy wykonywaniu operacji deszyfrowania ruchu.Urządzenie musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.Urządzenie musi posiadać dla deszyfrowania ruchu TLS 1.3 wsparcie dla X25519, X448 oraz minimum dla zestawów protokołów: TLS\_AES\_128\_GCM\_SHA256, TLS\_AES\_256\_GCM\_SHA384, TLS\_CHACHA20\_P0LY1305\_SHA256.Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji  w odniesieniu do źródłowego lub docelowego adresu IP.Urządzenie musi wspierać zarządzanie pasmem (QoS) i ustawienia dla aplikacji priorytetu oraz pasma.Urządzenie musi zapewniać inspekcję komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu blokowania tunelowania SSH.Urządzenie musi posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS/IDS musi być przechowywana na dostarczonych urządzeniach, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.Urządzenie musi posiadać bezpośrednio w GUI możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur oraz powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.Urządzenie musi posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na dostarczonych urządzeniach.Urządzenie musi posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół (co najmniej: http, http2, smtp, imap, pop3, ftp, smb). Baza sygnatur antywirusa musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż raz na 48 godzin i pochodzić od tego samego producenta co urządzenie.Urządzenie musi posiadać funkcję antispyware. Baza sygnatur musi być przechowywana na dostarczonych urządzeniach, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co urządzenie.Urządzenie musi posiadać funkcję filtrowania URL.Urządzenie musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (a nie tylko filtrującego) ruch w politykach bezpieczeństwa.Urządzenie musi posiadać funkcję filtrowania URL, aby zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.Urządzenie musi posiadać oddzielne kategorie URL dla zagrożeń typu malware, phishing, C&C, ransomware oraz ostatnio zarejestrowane domeny.Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania kategorii URL.Urządzenie musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sandbox” plików różnych typów (co najmniej: Windows Portable Executable (m.in. exe, dll), MacOS (MachO, DMG, PKG), Linux ELF, pdf, MS Office, JAR, APK, JS, VBS, PowerShell Script, BAT, HTA) w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować urządzenie sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze docelowym po ataku. Interwał aktualizacyjny to maksymalnie 2 godziny.Urządzenie musi mieć możliwość konfiguracji, jakiego rodzaju typy plików z listy wspieranych przez funkcję sandbox zostaną wysłane do skanowania przez zewnętrzne systemy realizujące funkcję sandbox.Urządzenie musi wykrywać i blokować zagrożenia DNS w ruchu przechodzącym przez dostarczone urządzenia bez potrzeby rekonfiguracji serwera DNS.Urządzenie musi realizować podstawową ochronę DNS w zakresie:1. wykrywania zapytań do domen złośliwych (baza domen musi pochodzić od producenta urządzenia),
2. możliwości skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing).

Urządzenie musi obsługiwać funkcję DNS proxy.Urządzenie musi obsługiwać podstawową funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta musi być realizowana z wykorzystaniem SSL oraz IPSec.Urządzenie musi realizować zaawansowaną ochronę DNS w zakresie: 1. wykrywania domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA),
2. wykrywanie domen dynamicznych Dynamic DNS,
3. wykrywania nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych.

Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.Urządzenie musi posiadać funkcjonalność pozwalającą na wysyłanie ruchu do narzędzi firm trzecich w celu dodatkowej analizy i detekcji zagrożeń.Urządzenie musi pracować jako para urządzeń wysokiej dostępności (HA) w trybach Active/Standby, Active/Active.Jeżeli w oferowanych urządzeniach, którekolwiek licencje/subskrypcje są czasowe, ograniczające w jakikolwiek sposób funkcjonalności, Zamawiający wymaga dostarczenia licencji/subskrypcji na okres 3 lat od daty podpisania protokołu zdawczo-odbiorczego. |  |  |
|  | Zarządzanie | Urządzenie musi być zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji (lub pobieranie) dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.Urządzenie musi być wyposażone w interfejs API (REST, JSON, XML) będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Nie jest dopuszczalne, aby istniała konieczność instalacji lub pobierania dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem. Jeżeli dostęp do API urządzenia, jego dokumentacji, zadawania pytań do pomocy, wymaga licencji lub subskrypcji - należy dostarczyć odpowiednie.Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż:1. bazy lokalnej,
2. serwera Radius,
3. serwera TACACS+,
4. serwera AD/LDAP,
5. dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH, a dla dostępu GUI za pomocą certyfikatów kryptograficznych.

Urządzenie musi posiadać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:1. LDAP,
2. Microsoft Active Directory,
3. Microsoft Exchange,
4. Syslog,
5. RADIUS,
6. TACACS+.

Dostęp i zarządzanie z sieci musi być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). Urządzenie musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.Urządzenie musi posiadać politykę kontroli dostępu, precyzyjnie definiującą prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, mających wspólny źródłowy adres IP, ustalanie tożsamości musi odbywać się również transparentnie.Urządzenie musi pozwalać na lokalne zbieranie (na niemechaniczne zasoby dyskowe w dostarczonych urządzeniach) i analizowanie logów, korelowanie zbieranych informacji oraz budowanie raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu URL, deszyfracji SSL.Urządzenie musi dostarczać predefiniowane przez producenta raporty standardowe, jak i umożliwiać tworzenie raportów niestandardowych.Urządzenie musi pozwalać na zapisanie raportów i ich uruchamianie w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.Urządzenie musi umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach, a proces oznaczania etykiet musi pozwalać na użycie:1. reakcji na zdarzenie/log (np. wystąpienie zagrożenia),
2. API.

Urządzenie musi posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP oraz etykietach (tagi) dla środowiska VMware ESX i VMware vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można następnie wykorzystywać w polityce bezpieczeństwa urządzeń. |  |  |
|  | Oprogramowanie klienckie VPN | Oprogramowanie klienckie w podstawowej funkcjonalności zdalnego dostępu VPN musi wspierać co najmniej poniższe systemy operacyjne:1. Windows 10, Windows 11,
2. macOS od wersji co najmniej 10.11.

Oprogramowanie klienckie Remote Access VPN musi posiadać wsparcie producenta (możliwość zakładania spraw w dziale wsparcia producenta). Jeśli wymaga to dodatkowych licencji/zakupów należy je dostarczyć.Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.Jeżeli oprogramowanie klienckie VPN jest dodatkowo licencjonowane przez producenta oraz wymaga odrębnego kontraktu serwisowego/supportowego, to wówczas należy to przewidzieć i dostarczyć odpowiednie licencje.Oprogramowanie klienckie VPN dla minimum 300 użytkowników. |  |  |
|  | Gwarancja/ Wsparcie producenta | Trzyletnia gwarancja/wsparcie producenta urządzeń z gwarantowanym czasem reakcji serwisu lub wysyłki części, najpóźniej w następnym dniu roboczym 9x5 (tzw. Next business day). Naprawa realizowana przez producenta urządzeń lub autoryzowany przez producenta serwis w miejscu eksploatacji.Możliwość aktualizacji i pobrania sterowników do oferowanego modelu urządzeń w najnowszych certyfikowanych wersjach, bezpośrednio z sieci Internet za pośrednictwem strony www producenta urządzeń.Telefoniczna linia techniczna producenta umożliwiająca zgłoszenie usterki sprzętowej urządzenia w czasie obowiązywania gwarancji/wsparcia producenta po podaniu numeru seryjnego urządzenia. |  |  |

1. **Wsparcie powdrożeniowe**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Opis** | ***Jednostka miary*** | ***Ilość*** |
|  | Wsparcie powdrożeniowe. | **Kpl.** | **1** |

1. **Dokumentacja**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Opis** | ***Jednostka miary*** | ***Ilość*** |
|  | Dokumentacja.  | **Kpl.** | **1** |

Za realizację przedmioty zamówienia opisanego w SWZ, oferujemy **cenę brutto:** ...................................... **zł**

słownie.................................................................................................................................................zł

(w tym podatek VAT ................ % tj. .............................................. zł),

- zgodnie z poniższą tabelą ceny ofertowej.

Tabela ceny ofertowej

|  |  |
| --- | --- |
| **Elementy składowe ceny ofertowej** | **Kwota brutto [PLN]** |
| System zapór sieciowych (2 urządzenia) wraz z licencjami/subskrypcjami aktywnymi w okresie od **podpisania protokołu zdawczo-odbiorczego do 04.06.2026 r.** |  |
| Wsparcie powdrożeniowe |  |
| Dokumentacja |  |
| Licencje/subskrypcje aktywne okresie od **05.06.2026 r. do zakończenia 3 letniego okresu wsparcia (liczonego od dnia podpisania protokołu).** |  |

**Funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (ML) aktualizowanych dynamicznie przez producenta (F1) (która będzie oceniana w kryterium oceny ofert)**

* oświadczamy, że oferowany przedmiot zamówienia **nie posiada** powyższej funkcjonalności (0 pkt)
* oświadczamy, że oferowany przedmiot zamówienia **posiada** powyższą funkcjonalność (15 pkt)

*Należy zaznaczyć X wybraną opcję.*

**Funkcjonalność zaawansowanej ochrony DNS w trybie rzeczywistym polegającej na pełnej analizie zapytania DNS przetwarzanego przez firewall (F2) (która będzie oceniana w kryterium oceny ofert)**

* oświadczamy, że oferowany przedmiot zamówienia **nie posiada** powyższej funkcjonalności (0 pkt)
* oświadczamy, że oferowany przedmiot zamówienia **posiada** powyższą funkcjonalność (15 pkt)

*Należy zaznaczyć X wybraną opcję.*

**Posiadanie przez oferowane urządzenia firewall konceptu konfiguracji kandydackiej (na poziomie API, GUI oraz CLI) (F3)” (które będzie oceniane w kryterium oceny ofert)**

* oświadczamy, że oferowane urządzenia firewall **nie posiadają** powyższego konceptu konfiguracji kandydackiej (0 pkt)
* oświadczamy, że oferowane urządzenia firewall **posiadają** powyższy koncept konfiguracji kandydackiej (10 pkt)

*Należy zaznaczyć X wybraną opcję.*

Oświadczamy, że powyższa cena zawiera wszystkie koszty jakie ponosi Zamawiający w przypadku wyboru niniejszej oferty.

Składamy niniejszą ofertę: w imieniu własnym[[1]](#footnote-1)\*/ jako Wykonawcy wspólnie ubiegający się o udzielenie zamówienia[[2]](#footnote-2)\*.

Ponadto oświadczamy, że będziemy odpowiadać solidarnie za wykonanie niniejszego zamówienia.

Przedmiot zamówienia wykonamy w terminie: **90 dni od podpisania umowy**.

Oświadczamy, że **zapoznaliśmy się z postanowieniami wzoru umowy**, załączonym do specyfikacji warunków zamówienia, **akceptujemy bez zastrzeżeń przedmiotowe postanowienia, w tym warunki płatności** i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszym wzorem i naszą ofertą.

Oświadczamy, że uważamy się za związanych niniejszą ofertą na **czas wskazany w SWZ.**

Oświadczamy, że przyjmujemy **warunki realizacji zamówienia określone w SWZ i w wyjaśnieniach do SWZ.**

Oświadczenie na temat polegania na zdolnościach innych podmiotów w celu spełnienia warunków udziału
w postępowaniu:

* polegam/y na zdolnościach innych podmiotów
* nie polegam/y na zdolnościach innych podmiotów.

Informuję, iż  **nie powierzymy** do wykonania podwykonawcom żadnej części niniejszego zamówienia\*.

Informujemy, iż następujące części niniejszego zamówienia **powierzymy** do wykonania wskazanym niżej podwykonawcom \*:

(\* niepotrzebne skreślić)

|  |  |
| --- | --- |
| Lp. | **Wykaz części zamówienia**, których realizację Wykonawca zamierza powierzyć podwykonawcom- z podaniem **firm podwykonawców**  |
| 1 |  |
| 2 |  |

Oświadczamy, że złożona oferta:

**□ nie prowadzi** do powstania u zamawiającego obowiązku podatkowego zgodniez przepisami
 o podatku od towarów i usług\*;

**□ prowadzi** do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisamio podatku od towarów i usług, jednocześnie wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku[[3]](#footnote-3)\*.

|  |  |  |
| --- | --- | --- |
| Nazwa (rodzaj) towaru lub usługi | Wartość bez kwoty podatku | Kwota podatku od towarów i usług, która powinna być doliczona do ceny złożonej oferty, o ile nie wynika toz treści złożonej oferty |
|  |  |  |
|  |  |  |

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane a art. 13 lub art. 14 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, str. 1), w skrócie „RODO”, wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w przedmiotowym postępowaniu.

Oświadczam, że podwykonawca/podmiot trzeci wypełnił obowiązki informacyjne przewidziane a art. 13 lub art. 14 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, str. 1), w skrócie „RODO”, wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał w celu ubiegania się o udzielenie zamówienia publicznego w przedmiotowym postępowaniu *(dotyczy w szczególności danych osobowych osoby/ób fizycznej/ych skierowanej/ych do realizacji zamówienia)*

*(zaznaczyć właściwe X)*:

🞏 tak

🞏 nie dotyczy,

Jestem/jesteśmy *(zaznaczyć właściwe X)*:

🞏 mikroprzedsiębiorstwem,

🞏 małym przedsiębiorstwem,

🞏 średnim przedsiębiorstwem.

*UWAGA:*

*- Mikroprzedsiębiorstwo to przedsiębiorstwo zatrudniające mniej niż 10 pracowników, którego roczny obrót oraz/lub całkowity bilans roczny nie przekracza 2 milionów euro.*

*- Małe przedsiębiorstwo to przedsiębiorstwo zatrudniające mniej niż 50 pracowników, którego roczny obrót oraz/lub całkowity bilans roczny nie przekracza 10 milionów euro.*

*- Średnie przedsiębiorstwo to przedsiębiorstwo zatrudniające mniej niż 250 pracowników, którego roczny obrót nie przekracza 50 milionów euro lub całkowity bilans roczny nie przekracza 43 milionów euro.*

Oferta została złożona na ............ stronach.

Integralną część oferty stanowią następujące dokumenty:

1. oświadczenie o którym mowa w art.125 ust.1 Pzp.
2. ……………………………………………

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa(y)Wykonawcy(ów) | Imię i nazwisko osoby(osób) upoważnionej(nych) do podpisania niniejszej oferty w imieniu Wykonawcy(ów) |
|  |  |  |
|  |  |  |

**Dokument przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.**

**Załącznik Nr 4 do SWZ – oświadczenie o braku podstaw do wykluczenia**

**i spełnienia warunków udziału w postępowaniu**

|  |  |
| --- | --- |
| Wykonawca:  | Zamawiający:**Gmina Nysa**Urząd Miejski w Nysieul. Kolejowa 15, 48-303 Nysa |
| NIP |  |

**Oświadczenie wykonawcy**

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych

##### Przystępując do udziału w postępowaniu o udzielenie zamówienia publicznego pn.:

**Wymiana systemu zapór sieciowych w Urzędzie Miejskim w Nysie,** *w ramach realizacji projektu Cyberbezpieczny Samorząd - Gmina Nysa (umowa o powierzenie grantu: FERC.02.02-CS.01-001/23/0675/ FERC.02.02-CS.01-001/23/2024 z 04.06.2024 r.)*

oświadczam, co następuje:

**OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:**

Oświadczam, że spełniam warunki udziału w postępowaniu określone w pkt .......SWZ.

Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust.1 ustawy Pzp.

Oświadczam, że nie podlegam wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 7 ust. 1 pkt. 1-3 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ……… ………………………………… ustawy *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 ustawy Pzp).*

Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy podjąłem następujące środki naprawcze:………………………………………………

**INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZASOBACH INNYCH PODMIOTÓW**:

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w specyfikacji warunków zamówienia*,* polegam na zasobach następującego/ych podmiotu/ów: ………………………………………………………………………….……………………………………………………,
w następującym zakresie: ……………………………………………………………………………

*(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu).*

**OŚWIADCZENIE DOTYCZĄCE PODWYKONAWCY NIEBĘDĄCEGO PODMIOTEM, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:**

Oświadczam, że w stosunku do następującego/ych podmiotu/tów, będącego/ych podwykonawcą/ami: ……………………………………………………………………..….…… *(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*, nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.

**OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:**

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne
i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

......................................................

(miejscowość i data )

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa(y)Wykonawcy(ów) | Imię i nazwisko osoby(osób) upoważnionej(nych) do podpisania niniejszej oferty w imieniu Wykonawcy(ów) |
|  |  |  |
|  |  |  |

**Dokument przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.**

|  |  |
| --- | --- |
| Nazwa podmiotu na którego zasoby powołuje się Wykonawca: | Zamawiający:**Gmina Nysa**Urząd Miejski w Nysieul. Kolejowa 15, 48-303 Nysa |
| NIP |  |

##### Postępowanie o udzielenie zamówienia publicznego pn.:

**Wymiana systemu zapór sieciowych w Urzędzie Miejskim w Nysie,** *w ramach realizacji projektu Cyberbezpieczny Samorząd - Gmina Nysa (umowa o powierzenie grantu: FERC.02.02-CS.01-001/23/0675/ FERC.02.02-CS.01-001/23/2024 z 04.06.2024 r.)*

**OŚWIADCZENIE PODMIOTU, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:**

Oświadczam, że w zakresie w jakim udostępniam zasoby, spełniam warunki udziału w postępowaniu określone
w pkt .......SWZ.

Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust.1 ustawy Pzp.

Oświadczam, że nie podlegam wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 7 ust. 1 pkt. 1-3 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ……… ………………………………… ustawy *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 ustawy Pzp).*

Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy podjąłem następujące środki naprawcze:………………………………………………

......................................................

(miejscowość i data )

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa(y)Wykonawcy(ów) | Imię i nazwisko osoby(osób) upoważnionej(nych) do podpisania niniejszej oferty w imieniu Wykonawcy(ów) |
|  |  |  |
|  |  |  |

**Dokument przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.**

**Załącznik Nr 5 do SWZ – wykaz wykonanych dostaw**

**Dokument składany na wezwanie o którym mowa w punkcie 22.2 SWZ.**

|  |  |
| --- | --- |
| Wykonawca:  | Zamawiający:**Gmina Nysa**Urząd Miejski w Nysieul. Kolejowa 15, 48-303 Nysa |

**WYKAZ WYKONANYCH DOSTAW**

##### Przystępując do udziału w postępowaniu o udzielenie zamówienia publicznego pn.:

**Wymiana systemu zapór sieciowych w Urzędzie Miejskim w Nysie,** *w ramach realizacji projektu Cyberbezpieczny Samorząd - Gmina Nysa (umowa o powierzenie grantu: FERC.02.02-CS.01-001/23/0675/ FERC.02.02-CS.01-001/23/2024 z 04.06.2024 r.)*

przedkładam/y **wykaz dostaw wykonanych**, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane, **wraz z załączeniem dowodów** określających, czy te dostawy zostały wykonanie należycie, *przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów - oświadczenie wykonawcy*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp. | Przedmiot zamówienia z określonym zakresem | Wartość brutto wykonanych dostaw wraz z wdrożeniem urządzeń typu firewall lub systemu zabezpieczeń firewall wraz z urządzeniami typu firewall | Data wykonania  | na rzecz jakiego podmiotu usługi były wykonane/ są wykonywane (Zamawiający) |
| **1** |  |  |  |  |
| **2** |  |  |  |  |

Oświadczam/my\*, że:

a) poz. ………… wykazu stanowi doświadczenie Wykonawcy/Wykonawców\* składającego ofertę,

b) poz. …………… wykazu jest doświadczeniem innych podmiotów, których zasoby zostaną oddane nam do dyspozycji na zasadach określonych w Pzp., na potwierdzenie czego załączam/y\* w szczególności pisemne zobowiązanie o którym mowa w SWZ

......................................................

(miejscowość i data)

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa(y)Wykonawcy(ów) | Imię i nazwisko osoby(osób) upoważnionej(nych) do podpisania niniejszej oferty w imieniu Wykonawcy(ów) |
|  |  |  |
|  |  |  |

**Dokument przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.**

 **Załącznik Nr 6 do SWZ – oświadczenie o przynależności lub braku przynależności**

**Dokument składany na wezwanie o którym mowa w punkcie 22.2 SWZ.**

|  |  |
| --- | --- |
| Wykonawca:  | Zamawiający:**Gmina Nysa**Urząd Miejski w Nysieul. Kolejowa 15, 48-303 Nysa |

**Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej
o której mowa w art. 108 ust.1 pkt. 5 Ustawy Pzp**

##### Przystępując do udziału w postępowaniu o udzielenie zamówienia publicznego pn.:

**Wymiana systemu zapór sieciowych w Urzędzie Miejskim w Nysie,** *w ramach realizacji projektu Cyberbezpieczny Samorząd - Gmina Nysa (umowa o powierzenie grantu: FERC.02.02-CS.01-001/23/0675/ FERC.02.02-CS.01-001/23/2024 z 04.06.2024 r.)*

oświadczam, że jako wykonawca:

 nie należę\* do grupy kapitałowej\*\*, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. 2024 poz. 1616)

 należę\* do grupy kapitałowej\*\*, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. 2024 poz. 1616), w której skład wchodzą następujące podmioty:

 1)………………………………………………………………………………………………

2)………………………………………………………………………………………………

 *( lub lista w załączeniu)*

***W przypadku przynależności do tej samej grupy kapitałowej wykonawca wraz z oświadczeniem składa* dokumenty lub informacje potwierdzające przygotowanie oferty, niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej**

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

......................................................

(miejscowość i data )

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa(y)Wykonawcy(ów) | Imię i nazwisko osoby(osób) upoważnionej(nych) do podpisania niniejszej oferty w imieniu Wykonawcy(ów) |
|  |  |  |
|  |  |  |

**Dokument przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.**

**Uwaga**

***\*****niepotrzebne skreślić*

**\*\****zgodnie z art. 4 pkt. 14 ustawy z dnia 16 lutego 2007r. o ochronie konkurencji i konsumentów (Dz.U. 2024 poz. 1616) przez grupę kapitałową rozumie się wszystkich przedsiębiorców, którzy są kontrolowani w sposób bezpośredni lub pośredni przez jednego przedsiębiorcę, w tym również tego przedsiębiorcę.*

**Załącznik Nr 7 do SWZ – oświadczenie o aktualności oświadczeń**

**Dokument składany na wezwanie o którym mowa w punkcie 22.2 SWZ.**

|  |  |
| --- | --- |
| Wykonawca:  | Zamawiający:**Gmina Nysa**Urząd Miejski w Nysieul. Kolejowa 15, 48-303 Nysa |

##### Przystępując do udziału w postępowaniu o udzielenie zamówienia publicznego pn.:

**Wymiana systemu zapór sieciowych w Urzędzie Miejskim w Nysie,** *w ramach realizacji projektu Cyberbezpieczny Samorząd - Gmina Nysa (umowa o powierzenie grantu: FERC.02.02-CS.01-001/23/0675/ FERC.02.02-CS.01-001/23/2024 z 04.06.2024 r.)*

Oświadczam, że informacje zawarte w złożonym przeze mnie oświadczeniu, o niepodleganiu wykluczeniu o którym mowa w art. 125 ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych, odnoszące się do podstaw wykluczenia z postępowania w zakresie określonym przez Zamawiającego w dokumentach zamówienia pozostają aktualne na dzień składania niniejszego oświadczenia.

......................................................

(miejscowość i data )

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa(y)Wykonawcy(ów) | Imię i nazwisko osoby(osób) upoważnionej(nych) do podpisania niniejszej oferty w imieniu Wykonawcy(ów) |
|  |  |  |
|  |  |  |

**Dokument przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.**

**Załącznik Nr 8 do SWZ – oświadczenie o którym mowa w art.117 ust. 4 Pzp.**

**Dokument składany na wezwanie o którym mowa w punkcie 22.2 SWZ.**

|  |  |
| --- | --- |
| Wykonawca:  | Zamawiający:**Gmina Nysa**Urząd Miejski w Nysieul. Kolejowa 15, 48-303 Nysa |

Oświadczenie składane na podstawie art. 117 ust. 4 ustawy z dnia 11 września 2019 r. – Prawo zamówień

##### Przystępując do udziału w postępowaniu o udzielenie zamówienia publicznego pn.:

**Wymiana systemu zapór sieciowych w Urzędzie Miejskim w Nysie,** *w ramach realizacji projektu Cyberbezpieczny Samorząd - Gmina Nysa (umowa o powierzenie grantu: FERC.02.02-CS.01-001/23/0675/ FERC.02.02-CS.01-001/23/2024 z 04.06.2024 r.)*

oświadczamy, że:

1. Wykonawca ………………………………………………………………………… zrealizuje następujące

 (nazwa i adres wykonawcy)

usługi/dostawy/roboty budowlane\*:…………………………………………………………………

1. Wykonawca ………………………………………………………………………… zrealizuje następujące

 (nazwa i adres wykonawcy)

usługi/dostawy/roboty budowlane\*:…………………………………………………………………

......................................................

(miejscowość i data )

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa(y)Wykonawcy(ów) | Imię i nazwisko osoby(osób) upoważnionej(nych) do podpisania niniejszej oferty w imieniu Wykonawcy(ów) |
|  |  |  |
|  |  |  |

**Dokument przekazuje się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.**

1. \* Niepotrzebne skreślić [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)
3. \* Niepotrzebne skreślić [↑](#footnote-ref-3)