pieczątka firmowa **Załącznik nr 1 do SIWZ**

...........dnia ............r.

# O F E R T A

na dostawę, konfiguracje i uruchomienie zestawu UTM

dla Sieci Badawczej Łukasiewicz-

 Przemysłowy Instytut Automatyki i Pomiarów PIAP

Postępowanie o udzielenie zamówienia publicznego w trybie

Przetargu nieograniczonego

Znak KZP/08/2020

## DANE WYKONAWCY

Nazwa...........................................................................................................................................

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

Adres............................................................................................................................................

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

Telefon..........................................................................................................................................

Fax................................................................................................................................................

E-mail...........................................................................................................................................

**I. Podstawowe informacje dotyczące oferty**

**Część 1**

1. Cena za dostawę, konfigurację i uruchomienie zestawu UTM w raz ze wsparciem technicznym na okres 3 lat oraz szkoleniem użytkowników urządzenia wraz z podatkiem VAT: złotych słownie.................................................................................................................................................................................................złotych).

2. Termin dostawy: ……………………dni kalendarzowych od podpisania umowy.

3. Okres gwarancji:

……………….. miesięcy (słownie ……………………….. miesięcy)

### II. Opis sposobu wykonania dostawy

Przez wykonanie dostawy rozumie się dostarczenie wszystkich elementów zamówienia zgodnie z zakresem określonym w pkt. III SIWZ wraz ze wsparciem technicznym oraz szkoleniem użytkowników urządzenia warunkach tam opisanych.

### GWARANCJA

Na wykonaną dostawę udzielam gwarancji na warunkach określonych w ofercie.

### III. Informacje dodatkowe

Informuję że następujące prace powierzę podwykonawcom\*) / żadnych prac nie powierzę podwykonawcom\*) …………………………………………..………………………..

………………………………………………………………………………………..

\*) *niepotrzebne skreślić.*

**IV. Oświadczenia Wykonawcy**

1. Oświadczam, że zapoznałem się ze Specyfikacją Istotnych Warunków Zamówienia i nie wnoszę do niej żadnych uwag.

2. Oświadczam, że zapoznałem się z projektem umowy i nie zgłaszam do niego żadnych zastrzeżeń.

3. Oświadczam, że akceptujemy warunki płatności przedstawione we wzorze umowy.

4. Oświadczam, że uważamy się za związanych niniejszą ofertą na okres 30 **dni** licząc od dnia otwarcia ofert (włącznie z tym dniem);

5. Oświadczam, że zobowiązujemy się do zawarcia umowy w miejscu i terminie wyznaczonym przez Zamawiającego;

6. **Oświadczam, że numer rachunku rozliczeniowego wskazany we wszystkich fakturach, które będą wystawione, jest rachunkiem/nie jest rachunkiem\*) dla którego zgodnie z Rozdziałem 3a ustawy z dnia 29 sierpnia 1997 r. - Prawo Bankowe (Dz. U. 2017.1876 ze zm.) prowadzony jest rachunek VAT.**

**7. Jeśli numer rachunku rozliczeniowego wskazany przez Wykonawcę, o którym mowa pkt.6 jest rachunkiem dla którego zgodnie z Rozdziałem 3a ustawy z dnia 29 sierpnia 1997 r. - Prawo Bankowe (Dz. U. 2017.1876 ze zm.) prowadzony jest rachunek VAT to:**

1. **Wykonawca oświadcza, że wyraża zgodę na dokonywanie przez Zamawiającego płatności systemie podzielonej płatności tzw. split payment.**

\*) *niepotrzebne skreślić.*

W załączeniu:

Załącznik 1 do oferty – Parametry oferowanego sprzętu

Załącznik 2 do oferty – Oświadczenie osób fizycznych w zakresie art. 24 ust.1 ustawy Pzp.

Załącznik 3 do oferty – Oświadczenie o przynależności do grupy kapitałowej

Oferta wraz z załącznikami zawiera łącznie ..........................ponumerowanych stron.

Podpis i pieczątka imienna

osoby upoważnionej do

reprezentowania firmy

Załącznik nr 1 do Oferty

#### Oferowany sprzęt

Uwaga: w kolumnie „oferowane” należy wpisać konkretne wartości parametrów oferowanego sprzętu.

**Oferowany typ / model: ……………..**

**Producent: ………………**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

|  |  |
| --- | --- |
| **Parametr** | **Oferowany** |
| Funkcje modułu Firewall1. System realizujący funkcję Firewall musi zostać dostarczony w postaci klastra pracującego w trybie Active-Passive składającego się z dwóch urządzeń.
2. Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
3. Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
4. Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.
5. Musi obsługiwać Multicast routing.
6. Musi obsługiwać Policy Based routing.
7. Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.
8. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
9. Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.
10. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
11. Musi obsługiwać Dynamic DNS.
12. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
13. Musi obsługiwać translację portów: PAT.
14. Musi obsługiwać IPSec NAT traversal.
15. Musi obsługiwać mechanizm Policy Based NAT.
16. Musi obsługiwać VLAN 802.1Q.
17. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
18. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
19. Musi mieć możliwość obsługi zapasowego łącza typu LTE poprzez podłączenie zewnętrznego modemu USB.
20. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
21. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.
22. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza.
23. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
24. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
25. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.
26. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.
27. Urządzenie musi posiadać co najmniej 4 mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Active Directory.
28. Co najmniej dwie metody transparentnej autoryzacji nie wymagają instalacji dedykowanego

agenta na stacjach roboczych użytkowników. 1. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.
2. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
3. Musi dostarczać mechanizmów identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
4. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
5. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
6. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.
7. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
8. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.
9. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.
10. Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
11. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.
12. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.
 |  |
| Dostarczony system bezpieczeństwa musi zapewniać:1. Ochronę z wykorzystaniem mechanizmów IPS.
2. Ochronę antywirusową.
3. Ochronę przed nieznanymi zagrożeniami.
4. Ochronę przed phishingiem.
5. Ochronę przed niechcianą pocztą.
6. Kontrolę wykorzystywanych aplikacji.
7. Możliwość filtrowania URL.
 |  |
| Parametry fizyczne systemu Firewall:Element systemu pełniący funkcję Firewall musi dysponować :* 8 portami 1Gb RJ45.
* System musi umożliwiać rozbudowę o dodatkowe porty: 4 x porty optyczne 10G lub

8 x porty optyczne 1G lub 8 x porty miedziane 1G .* Minimum 4 GB pamięci RAM.
* Minimum 2 porty USB 3.0.
* Minimum jeden port typu Console.
* Minimalna temperatura pracy urządzenia od 0 do 40 stopni Celsjusza.
 |  |
| Parametry wydajnościowe systemu:* Przepustowość Firewall minimum: 19.6 Gbps.
* Przepustowość IPSec VPN nie mniejsza niż: 5.2 Gbps.
* Przepustowość skanowania antywirusowego nie mniejsza niż: 3.5 Gbps.
* Przepustowość w ramach ochrony przed atakami nie mniejsza niż: 5.7 Gbps.
* Przepustowość systemu z włączonymi mechanizmami skanowania antywirusowego, ochrony przed atakami, kontroli aplikacji minimum: 3.1 Gbps.
* Obsługa nie mniej niż: 250 tuneli IPSec site-to-site.
* Obsługa nie mniej niż: 250 tuneli client-to-site.
* Obsługa nie mniej niż: 3.800.000 jednoczesnych połączeń.
* Obsługa nie mniej niż: 82.000 nowych połączeń na sekundę.
* W ramach Firewall system musi obsługiwać minimum: 300 sieci VLAN.
 |  |
| W ramach ochrony przed atakami system musi zapewniać:1. Automatyczną aktualizację bazy sygnatur IPS. Musi ona zawierać co najmniej 8000 definicji sygnatur.
2. Automatyczne blokowanie znanych źródeł ataków.
3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).
5. Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer OverFlow, Remote File Inclusions.
6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.
 |  |
| W ramach kontroli antywirusowej system musi zapewniać:1. Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie lub system musi posiadać mechanizmy integracji z drugim zewnętrznym skanerem działającym lokalnie. W przypadku skanera zewnętrznego koniecznym jest dostarczenie pełnej dokumentacji przykładowego systemu oraz wykazanie w testach poprawności działania takiej integracji z zewnętrznym skanerem lokalnym.
2. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.
3. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.
4. Możliwość skanowania plików o rozmiarze co najmniej 20MB.
5. Możliwość zdefiniowania rozmiaru skanowanego pliku.
6. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
7. Ilość sygnatur w ramach skanera sygnaturowego nie może być mniejsza niż 2.500.000.
8. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
9. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.
10. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.
 |  |
| W ramach ochrony przed nieznanymi zagrożeniami system musi zapewniać:1. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję analizy behawioralnej w oparciu o platformę typu sandbox, w tym co najmniej:
* W tym zakresie system musi pracować w trybie lokalnym lub z wykorzystaniem mechanizmów chmury (w granicach Unii Europejskiej).
* Analizę plików pobieranych przez HTTP/HTTPS i przesyłanych pocztą elektroniczną (SMTP, POP3, IMAP) oraz plików pobieranych za pomocą protokołu FTP.
* Ogólne oszacowanie poziomu ryzyka dla analizowanych plików i określanie różnego rodzaju akcji na ich podstawie.
* Kwarantannę podejrzanych plików co najmniej dla protokołu SMTP.
* Możliwość blokowania wiadomości e-mail przesyłanej protokołem SMTP zawierającej podejrzane załączniki do czasu zakończenia ich analizy.
* Możliwość analizy plików o rozmiarze co najmniej 10MB.
* Brak ograniczeń co do ilości analizowanych plików.
 |  |
| W ramach ochrony przed phishingiem system musi zapewniać:1. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję ochrony przed phishingiem, w tym co najmniej:
* Możliwość blokowania dostępu do spreparowanych stron.
* Ochronę przed phishingiem nie zależnie od typu połączenia, protokołu, portu.
* Możliwość tworzenia białych/czarnych list domen, do których połączenia będą filtrowanie.
* Notyfikację użytkownika, którego dotyczy zdarzenie - niezależnie od logów i raportów.
* Kontrolę zapytań DNS.
 |  |
| W ramach kontroli antyspamowej system musi zapewniać:1. Analizę wiadomości pocztowych w oparciu o technologię Recurrent Pattern Detection.
2. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.
3. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
4. Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
5. Możliwość tworzenia białych/czarnych list, w oparciu o które system zezwala lub odmawia wysyłania wiadomości e-mail dla określonych nadawców i odbiorców.
6. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail
 |  |
| W ramach filtrowania zawartości URL system musi zapewniać:1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
2. Baza filtra url musi zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
3. Baza URL musi zawierać co najmniej 14.000.000 skategoryzowanych stron www.
4. Odpytywanie bazy on-line w czasie rzeczywistym.
5. Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym dlaczego dostęp do strony www został zablokowany.
6. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
7. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
8. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.
9. Możliwość określania reputacji adresu URL i na podstawie reputacji podejmowanie określonych akcji.
10. Możliwość filtrowania treści w oparciu o typy MIME.
11. Możliwość blokowania plików cookies dla określonych domen.
12. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
13. Analizę treści dla protokołu https.
14. Wyłączenie inspekcji https dla wybranych kategorii stron www.
 |  |
| W ramach kontroli aplikacyjnej system musi zapewniać:1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
2. Ilość rozpoznawanych aplikacji: nie mniej niż 1800, podzielonych na kategorie.
3. W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
4. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.
5. Możliwość ograniczania wykorzystywanej przepustowości aplikacji lub kategorii aplikacji.
 |  |
| Wymagane funkcje VPN systemu:1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
5. Obsługa Dead Peer Detection (DPD).
6. Wsparcie dla IKEv1 i IKEv2.
7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.
10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.
12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.
13. Musi umożliwiać uruchomienie portalu SSL VPN, który umożliwia autoryzację w oparciu o protokoły RADIUS, LDAP, Active Directory, lokalną bazę użytkowników.
14. Portal SSL VPN musi zapewniać wsparcie dla protokołów: SSH, RDP, HTTP.
15. Portal SSL VPN musi wspierać funkcjonalność Single-Sign-On dla aplikacji webowych w oparciu o protokół SAML.
 |  |
| Zarządzanie1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.
8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.
 |  |
| Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania:1. Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
2. Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
3. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
4. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według zdefiniowanego harmonogramu.
5. Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
6. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję porównywania różnych wersji konfiguracji. W ramach postępowania muszą zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
7. Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania muszą zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
8. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
9. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
10. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
11. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
12. Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
13. Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
14. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
15. Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
16. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
17. System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.
18. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
19. Musi być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
20. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
21. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
22. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
23. Rozwiązanie nie może narzucać ograniczeń, co do czasu przechowywania logów.
 |  |
| Licencje i wsparcie techniczne1. W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Muszą one obejmować:
* Ochrona przed atakami (IPS), Kontrola aplikacji, Web Filtering, Antyspam, Antywirus, Bazy reputacyjne adresów, Rozpoznawanie urządzeń pracujących w sieci, Ochrona przed nieznanymi zagrożeniami, Ochrona przed phishingiem, – na okres 3 lat.
1. System musi być objęty serwisem gwarancyjnym producenta przez okres 3 lat, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7 (świadczone telefonicznie lub poprzez portal).
 |  |

**Cena brutto za całość przedmiotu Zamówienia:**

**…………………………………………………**

Załącznik nr 2 do oferty

**OŚWIADCZENIE O BRAKU PODSTAW DO WYKLUCZENIA / I SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU**

……………………

 miejscowość, data

**OŚWIADCZENIE**

Przystępując do postępowania o udzielenie zamówienia publicznego nr KZP/05/2020

**Ja niżej podpisany**

**……………………………………………………………………………………**

**(imię i nazwisko)**

**Reprezentujący firmę** …………………………………………………………..

**(nazwa podmiotu)**

**Oświadczam, że na dzień składania ofert nie podlegam wykluczeniu z postępowania i spełniam warunki udziału w postępowaniu.**

**W przedmiotowym postępowaniu Zamawiający zgodnie z art. 24 ust. 1 pkt. 12-23 ustawy PZP wykluczy:**

**1.  wykonawcę, który nie wykazał spełniania warunków udziału w postępowaniu lub nie został zaproszony do negocjacji lub złożenia ofert wstępnych albo ofert, lub nie wykazał braku podstaw wykluczenia;**

**2   wykonawcę będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:**

**a) o którym mowa w­ art. 165a, art. 181–188, art. 189a, art. 218–221, art. 228–230a, art. 250a, art. 258 lub art. 270–309 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. poz. 553, z późn. zm.) lub­ art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2016 r. poz. 176),**

**b) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny,**

**c)   skarbowe,**

**d) o którym mowa w art. 9 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769);**

**3.    wykonawcę, jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 13;**

**4.   wykonawcę, wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, chyba że wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;**

**5.  wykonawcę, który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawieniu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub obiektywne i niedyskryminacyjne kryteria, zwane dalej „kryteriami selekcji”, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych dokumentów;**

**6.  wykonawcę, który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd zamawiającego, mogące mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia;**

**7.  wykonawcę, który bezprawnie wpływał lub próbował wpłynąć na czynności zamawiającego lub pozyskać informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;**

**8.  wykonawcę, który brał udział w przygotowaniu postępowania o udzielenie zamówienia lub którego pracownik, a także osoba wykonująca pracę na podstawie umowy zlecenia, o dzieło, agencyjnej lub innej umowy o świadczenie usług, brał udział w przygotowaniu takiego postępowania, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu;**

**9.   wykonawcę, który z innymi wykonawcami zawarł porozumienie mające na celu zakłócenie konkurencji między wykonawcami w postępowaniu o udzielenie zamówienia, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;**

**10.  wykonawcę będącego podmiotem zbiorowym, wobec którego sąd orzekł zakaz ubiegania się o zamówienia publiczne na podstawie ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz. U. z 2015 r. poz. 1212, 1844 i 1855 oraz z 2016 r. poz. 437 i 544);**

**11.   wykonawcę, wobec którego orzeczono tytułem środka zapobiegawczego zakaz ubiegania się o zamówienia publiczne;**

**12.   wykonawców, którzy należąc do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2015 r. poz. 184, 1618 i 1634), złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że istniejące między nimi powiązania**  **nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.**

**Ponadto zamawiający przewiduje możliwość wykluczenia wykonawcy w sytuacji:**

**1.   w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. z 2015 r. poz. 978, 1259, 1513, 1830 i 1844 oraz z 2016 r. poz. 615) lub którego upadłość ogłoszono, z wyjątkiem wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz. U. z 2015 r. poz. 233, 978, 1166, 1259 i 1844 oraz z 2016 r. poz. 615);**

**2.  który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;**

**3.  jeżeli wykonawca lub osoby, o których mowa w ust. 1 pkt 14, uprawnione do reprezentowania wykonawcy pozostają w relacjach określonych w art. 17 ust. 1 pkt 2–4 z:**

**a) zamawiającym,**

**b) osobami uprawnionymi do reprezentowania zamawiającego,**

**c)   członkami komisji przetargowej,**

**d) osobami, które złożyły oświadczenie, o którym mowa w art. 17 ust. 2a**

–**chyba że jest możliwe zapewnienie bezstronności po stronie zamawiającego w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu;**

**4.  który, z przyczyn leżących po jego stronie, nie wykonał albo nienależycie wykonał w istotnym stopniu wcześniejszą umowę w sprawie zamówienia publicznego lub umowę koncesji, zawartą z zamawiającym, o którym mowa w art. 3 ust. 1 pkt 1–4, co doprowadziło do rozwiązania umowy lub zasądzenia odszkodowania;**

**5.  będącego osobą fizyczną, którego prawomocnie skazano za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny nie niższą niż 3000 złotych;**

**6.  jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za wykroczenie, o którym mowa w pkt 5;**

**7.  wobec którego wydano ostateczną decyzję administracyjną o naruszeniu obowiązków wynikających z przepisów prawa pracy, prawa ochrony środowiska lub przepisów o zabezpieczeniu społecznym, jeżeli wymierzono tą decyzją karę pieniężną nie niższą niż 3000 złotych;**

**8.  który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych, z wyjątkiem przypadku, o którym mowa w ust. 1 pkt 15, chyba że wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności.**

**Ponadto oświadczam, że spełniam warunki udziału w postępowaniu dotyczące:**

1. **kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów.**
2. **sytuacji ekonomicznej lub finansowej**
3. **zdolności technicznej lub zawodowej**

**Informacja w związku z poleganiem na zasobach innych podmiotów**

**Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w rozdz. V SIWZ polegam na zasobach następującego/ych podmiotu/ów:**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

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

**Oświadczenie dotyczące podmiotu, na którego zasoby powołuje się wykonawca**

**Oświadczam, że w stosunku do następującego/ych podmiotu/tów, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.:** ……………………………………………………………*(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 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.**

………………………………………

podpis Wykonawcy lub osoby/osób upoważnionej/ych do reprezentowania

*Dokument, który Wykonawca zobowiązany jest złożyć w terminie 3 dni od dnia zamieszczenia na stronie internetowej Zamawiającego informacji, o której mowa w art. 86 ust. 5*

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

Nazwa (firma) Wykonawcy albo Wykonawców ubiegających się wspólnie o udzielenie zamówienia

**OŚWIADCZENIE O GRUPIE KAPITAŁOWEJ**

My, niżej podpisani, działając w imieniu i na rzecz:

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

*(nazwa /firma/ i adres Wykonawcy/ Wykonawców wspólnie ubiegających się o udzielenie zamówienia)*

niniejszym oświadczamy, że ubiegając się o zamówienie publiczne na:

***Na dostawę zestawu UTM***

KZP/08/2020

* należymy do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2018 r. poz. 1986 z późn. zm), w skład której wchodzą następujące podmioty: ……………………………….\*
* nie należymy do grupy kapitałowej\*

\* zaznaczyć odpowiednie

…………………., dnia ……………………. …………………….

(miejscowość) (podpis i pieczątka uprawomocnionego przedstawiciela Wykonawcy

**Oświadczenie wykonawcy w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO**

**Oświadczenie należy złożyć wraz z ofertą**

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

 ……………………..

 Podpis i pieczątka imienna

osoby upoważnionej do

reprezentowania firmy