MGOPS
PIASECZNO

Piaseczno, 28.09.2022 r.

AD.230.101.2022.JD

Zapytanie ofertowe do kwoty 129 999,99 złotych (netto)

Wobec treści art. 2 ust. 1 pkt. 1 Ustawy z dnia 11 września 2019 r. – Prawo Zamówień Publicznych (t.j Dz.U. 2022, poz.1710 z późn. zm.) zwracamy się z uprzejmą prośbą o przedstawienie oferty cenowej na usługę pn.: **„zakup dwóch sztuk Firewalla z licencjami subskrypcji pozwalającej na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 2 lat wraz z usługą instalacji dla każdego, dla Miejsko-Gminnego Ośrodka Pomocy Społecznej w Piasecznie , przy ul. Świętojańskiej 5A."**

Zamawiający: **Gmina Piaseczno**
ul. Kościuszki 5
05-500 Piaseczno
NIP: 123 12 10 962

Odbiorca: **Miejsko-Gminny Ośrodek Pomocy Społecznej**
ul. Świętojańska 5A
05-500 Piaseczno

NIP: 123-07-15-884
tel:(22)750-33-08, (22)756-52-73
e-mail: sekretariat@mgops.piaseczno.eu

1.PRZEDMIOT ZAMÓWIENIA:

Zakup 1 sztuki Firewalla obsługującego min. 1 500 000 (MGOPS) i 1 sztuki Firewalla obsługującego min. 1 250 000 (DDPS) połączeń jednocześnie wraz z licencjami subskrypcji pozwalającej na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 2 lat wraz usługą instalacji dla każdego.

Szczegółowy opis przedmiotu zamówienia zawiera Załącznika nr.1A i Załącznik 1B

2.TERMIN I SPOSÓB ZŁOŻENIA OFERTY:

1) Ofertę należy sporządzić na załączonym Formularzu Ofertowym stanowiącym załącznik nr 1.
2) Sporządzoną ofertę należy złożyć do dnia **05.10.2022r.** na adres e-mail **sekretariat@mgops.piaseczno.eu**
3) W związku z formą elektroniczną postępowania konieczne są skany podpisanych dokumentów.
4) Ofertę należy sporządzić w języku polskim. Oferta winna być podpisana przez osobę upoważnioną (kopia upoważnienia lub pełnomocnictwa).

5) Oferty złożone po terminie, nie będą rozpatrywane.
6) Zamawiający będzie rozpatrywał oferty złożone zgodnie z ogłoszeniem.
7) Wszelkie negatywne konsekwencje mogące wyniknąć z nierzetelnego przygotowania oferty(w tym nieczytelne) obciążają Wykonawcę.
8) Po otwarciu ofert i wyborze najkorzystniejszej oferty, w przypadku braku decyzji o unieważnieniu, Zamawiający sporządzi protokół z przeprowadzonego postępowania oraz podpisze z Wykonawcą umowę na realizację zadania.
9) Informacja o wyborze Wykonawcy, zostanie wysłana do Wykonawców, którzy odpowiedzieli na ogłoszenie.
10) Zamawiający może zamknąć postępowanie bez wyboru oferty w przypadku, gdy żadna oferta nie odpowiada warunkom określonym w zapytaniu lub gdy cena przekracza możliwości finansowe Zamawiającego.
11) Zamawiający zastrzega sobie prawo do unieważnienia przedmiotowego zapytania ofertowego na każdym jego etapie bez podania przyczyny.
12) Zamawiający może w każdym czasie, przed upływem terminu składania ofert, zmienić treść niniejszego zapytania ofertowego. Dokonane w ten sposób uzupełnienie stanie się integralną częścią zapytania.
13) Zamawiający zastrzega sobie prawo, że jeżeli cena najkorzystniejszej oferty przekroczy możliwości finansowe Zamawiającego, może on zmniejszyć przedmiot zamówienia.
14) W przypadku uchylenia się wybranego Wykonawcy od podpisania umowy, umowa zostanie zawarta z Wykonawcą, którego oferta jako kolejna spośród pozostałych jest najkorzystniejsza.
15) W sprawach nieuregulowanych w niniejszym zapytaniu mają zastosowanie przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2022 r., poz. 1360, z późn. zm.).

3.KRYTERIUM OCENY OFERT:

1) Ocena złożonych ofert będzie dokonana w oparciu o kryterium najniższej ceny.
2) Do realizacji zamówienia zostanie wybrany Wykonawca, który zaoferuje wykonanie przedmiotu zamówienia zgodnie z wymogami Zamawiającego i zaproponuje najniższą cenę całkowitą za całość usługi.
3) Zamawiający nie dopuszcza składania ofert częściowych.
4) W przypadku dwóch lub więcej ofert z taką samą ceną, Zamawiający wezwie pisemnie tych Wykonawców do złożenia ofert dodatkowych. Ceny ofert dodatkowych nie mogą być wyższe od ceny podanej w pierwszej ofercie.
5) Cena brutto oferty powinna zawierać wszystkie koszty, jakie Zamawiający będzie musiał ponieść przy realizacji zamówienia z uwzględnieniem podatku od towarów i usług VAT, kosztów transportu do siedziby Zamawiającego, innych opłat i podatków.

4. TERMIN REALIZACJI ZAMÓWIENIA:

Wykonawca będzie zobowiązany do realizacji zamówienia od dnia zawarcia umowy do **15.10.2022r.**

5. DOKUMENTY JAKIE POWINIEN WYKONAWCA DOŁĄCZYĆ DO OFERTY:

1) Wypełniony formularz ofertowy (Załącznik nr 1)
2) Oświadczenie oferenta (Załącznik nr 2)
3) Klauzula informacyjna RODO (Załącznik nr 3)

4) Odpis z właściwego rejestru lub CEIDG lub wpis świadczący o wykonywaniu usług będących przedmiotem zamówienia.
5) Wypełnioną specyfikację- Załącznik nr.1A i Załącznik nr.1B

6. OSOBA DO KONTAKTU ZE STRONY ZAMAWIAJĄCEGO

Przemysław Swatek – informatyk, Joanna Drążkiewicz -podinspektor
tel. (22) 756 72 63
e-mail: informatyk@mgops.piaseczno.eu, sekretariat@mgops.piaseczno.eu

Załączniki:

1. Formularz ofertowy (Załącznik nr 1)
2. Oświadczenie Oferenta (Załącznik nr 2)
3. Klauzula informacyjna RODO (Załącznik nr 3)
4. Specyfikacja przedmiotu zamówienia (Załącznik nr 1A i Załącznik nr.1B)

Zastępca Dyrektora
Miejsko-Gminnego Ośrodka
Pomocy Społecznej w Piasecznie
mgr Elżbieta Klimkowska

Załącznik Nr 1 do zapytania ofertowego

.....

(miejscowość i data)

Miejsko-Gminny
Ośrodek Pomocy Społecznej
ul. Świętojańska 5a
05-500 Piaseczno

Formularz ofertowy

Nazwa i siedziba Wykonawcy

.....

NIP.....

Tel.....

Fax.....

W odpowiedzi na zapytanie ofertowe nr **AD.230.101.2022.JD** z dnia **28.09.2022r.** pn. **„zakup dwóch sztuk Firewalla z licencjami subskrypcji pozwalającej na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 2 lat wraz z usługą instalacji dla każdego, dla Miejsko-Gminnego Ośrodka Pomocy Społecznej w Piasecznie , przy ul. Świętojańskiej 5A."**
oferujemy realizację zamówienia za całkowitą cenę:

Cena netto .....

Podatek Vat .....

Cena brutto .....

1. Zapoznaliśmy się z treścią zapytania ofertowego dla niniejszego zamówienia i nie wnosimy do niego zastrzeżeń oraz zdobyliśmy konieczne informacje do przygotowania oferty.
2. Gwarantujemy wykonanie całości zamówienia zgodnie z treścią zapytania ofertowego. Oświadczam/y, że oferowana cena zawiera wszystkie koszty związane z realizacją przedmiotu zamówienia.
3. Zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy na warunkach wymienionych w zapytaniu ofertowym, w miejscu i terminie wyznaczonym przez Zamawiającego.
4. Akceptujemy termin realizacji zamówienia określony w zapytaniu ofertowym.
5. Posiadamy uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania.
6. Posiadamy wiedzę i doświadczenie niezbędne do realizacji zamówienia.

7. Dysponujemy odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia.
8. Jesteśmy w dobrej sytuacji ekonomicznej i finansowej pozwalającej na rzetelne wykonanie przedmiotu umowy.
9. Nie otwarto wobec nas likwidacji lub nie ogłoszono upadłości.
10. Oświadczamy, że posiadamy ubezpieczenie OC w zakresie prowadzonej działalności, której niniejsze postępowanie dotyczy.
11. Załącznikami do niniejszego formularza stanowiącymi integralną część oferty są:

    1) .....

    2) .....

    3) .....

12. Oferta została złożona na ..... stronach podpisanych i kolejno ponumerowanych od nr ..... do nr ..... .
14. Osoba uprawniona do kontaktów w sprawie oferty ze strony oferenta:

Imię i nazwisko:.....
nr tel.: ..... adres e –mail .....

....

miejscowość , dnia *podpis upoważnionego przedstawiciela Wykonawcy*

Załącznik Nr 2 do zapytania ofertowego

OŚWIADCZENIE O SPEŁNIENIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Nazwa Wykonawcy	
Siedziba, adres Wykonawcy	
Tel./fax	
E-mail	

Przystępując do udziału w postępowaniu prowadzonym w trybie zapytania ofertowego na zamówienie pn.: **„zakup dwóch sztuk Firewalla z licencjami subskrypcji pozwalającej na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 2 lat wraz z usługą instalacji dla każdego, dla Miejsko-Gminnego Ośrodka Pomocy Społecznej w Piasecznie , przy ul. Świętojańskiej 5A.”**znak sprawy: AD.230.101.2022.JD z dn. 28.09.2022 r.

Oświadczam/y,
że Wykonawca spełnia warunki dotyczące:

- posiadania uprawnień do wykonywania określonej działalności lub czynności związanej z przedmiotem zapytania ofertowego, jeżeli przepisy prawa nakładają obowiązek ich posiadania;
- posiadania odpowiedniej wiedzy i doświadczenia, niezbędnych do prawidłowego wykonania usługi;
- dysponowania odpowiednim potencjałem technicznym, niezbędnym do prawidłowej realizacji zamówienia;
- dysponowania odpowiednimi osobami, zdolnymi do prawidłowej realizacji zamówienia;
- pozostawania w sytuacji ekonomicznej i finansowej, pozwalającej na prawidłowe wykonanie zamówienia,
- spełnienia warunków określonych w opisie przedmiotu zamówienia.

Uprzedzeni o odpowiedzialności z art. 233 Kodeksu Karnego oświadczam(y), że wszystkie podane wyżej informacje są zgodne z prawdą.

.....
Data i czytelny podpis

Załącznik Nr 3 do zapytania ofertowego

Klauzula informacyjna z art. 13 RODO do zastosowania w celu związanym z postępowaniem o udzielenie zamówienia publicznego

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

- Administratorem Pani/Pana danych osobowych jest Miejsko-Gminny Ośrodek Pomocy Społecznej w Piasecznie, ul Świętojańska 5 A, 05-500 Piaseczno, tel. (22) 737-23-97 lub (22) 756-72-63, adres e-mail: sekretariat@mgops.piaseczno.eu,

- kontakt z inspektorem ochrony danych osobowych pod adresem e-mail: iod@mgops.piaseczno.pl,

- Państwa dane będą przetwarzane w celu związanym z postępowaniem o udzielenie zamówienia publicznego – prowadzonego w trybie zapytania ofertowego pn. **„zakup dwóch sztuk Firewalla z licencjami subskrypcji pozwalającej na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 2 lat wraz z usługą instalacji dla każdego, dla Miejsko-Gminnego Ośrodka Pomoc Społecznej w Piasecznie , przy ul. Świętojańskiej 5A."**
znak sprawy: AD.230.101.2022.JD z dn. 28.09.2022 r. Podstawa prawną ich przetwarzania jest Państwa zgoda wyrażona poprzez akt uczestnictwa w postępowaniu oraz następujące przepisy prawa:

1. ustawa z dnia 11 września 2019 r. roku Prawo zamówień publicznych (t.j. Dz. U. z 2022 r. poz. 1710 z póź.zm.),
2. Rozporządzenie Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz. U. z 2020 r. poz. 2415),
3. ustawa o Narodowym zasobie archiwalnym i archiwach (t.j. Dz.U. 2020 r. poz. 164.).

- Państwa dane pozyskane w związku z postępowaniem o udzielenie zamówienia publicznego przetwarzane będą przez okres 5 lat od dnia zakończenia postępowania o udzielenie zamówienia.
- Państwa dane pozyskane w związku z postępowaniem o udzielenie zamówienia publicznego przekazywane będą wszystkim zainteresowanym podmiotom i osobom, gdyż co do zasady postępowanie o udzielenie zamówienia publicznego jest jawne.

1. - Ograniczenie dostępu do Państwa danych o których mowa wyżej może wystąpić jedynie w szczególnych przypadkach jeśli jest to uzasadnione ochroną prywatności zgodnie z art. 18 ustawy z dnia 11 września 2019 r. roku Prawo zamówień publicznych (t.j. Dz. U. z 2022 r. poz. 1710 z póź.zm.),

- Ponadto odbiorcą danych zawartych w dokumentach związanych z postępowaniem o zamówienie publiczne mogą być podmioty z którymi Miejsko-Gminny Ośrodek Pomocy Społecznej w Piasecznie zawarł umowy lub porozumienie w związku ze świadczeniem usług wsparcia technicznego i usuwaniem awarii. Odbiorców tych obowiązuje klauzula zachowania poufności pozyskanych w takich okolicznościach wszelkich danych, w tym danych osobowych.
- W odniesieniu do danych pozyskanych w związku z prowadzonym postępowaniem o udzielenie zamówienia publicznego przysługują Państwu następujące uprawnienia:

- prawo dostępu do swoich danych oraz otrzymania ich kopii;
- prawo do sprostowania (poprawiania) swoich danych;
- prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
- prawo do ograniczenia przetwarzania danych, przy czym przepisy odrębne mogą wyłączyć możliwość skorzystania z tego praw;
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych. Aby skorzystać z powyższych praw, należy się skontaktować z nami lub z naszym inspektorem ochrony danych.

4. - Podanie danych osobowych w związku udziałem w postępowaniu o zamówienia publiczne nie jest obowiązkowe, ale jest warunkiem niezbędnym do wzięcia w nim udziału. Wynika to stąd, że w zależności od przedmiotu zamówienia, zamawiający może żądać ich podania na podstawie przepisów dnia 11 września 2019 r. roku Prawo zamówień publicznych (t.j. Dz. U. z 2022 r. poz. 1710 z póź.zm.), oraz wydanych do niej przepisów wykonawczych, a w szczególności na podstawie Rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz. U. z 2020 r. poz. 2415).

.....

(data i podpis)

Firewall – 1 szt.			
Kwota jednostkowa netto [PLN]	Kwota jednostkowa brutto [PLN]	Koszt netto [PLN]	Koszt brutto [PLN]

Komponent	**Minimalne wymagania**
Wymagania ogólne	Zapora sieciowa typu Next Generation Firewall (NGFW)
	Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku
	Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić)
	Funkcja NAT oparta o reguły bezpieczeństwa
	NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe)
	System musi pochodzić z oficjalnej dystrybucji producenta
Ilość urządzeń	1 sztuka
Interfejsy sieciowe Wbudowane i dodatkowe	3 interfejsów 10 GbE SFP+
	16 interfejsy RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa
	2 interfejsy USB 3.0 dla przyszłych potrzeb i do podłączenia modemu 3G
	1 interfejs konsoli do zarządzania zaporą
	1 interfejs RJ-45 Ethernet 10/100/1000 do zarządzania zaporą
	Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa

	Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji
	Możliwość utworzenia przynajmniej 256 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q
	Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej
Dysk	Zapora powinna posiadać dysk M.2 o pojemności przynajmniej 64 GB z możliwością wymiany na większy
Parametry Wydajnościowe	Minimalna ilość jednocześnie obsługiwanych połączeń: 1 500 000,
	Możliwość obsłużenia przynajmniej 21 500 nowych połączeń w ciągu 1 sekundy
	Przepustowość urządzenia pracującego w trybie stateful firewall: 5,2 Gbps – dla ramki 1518B zgodnie z RFC 2544,
	Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 3.4 Gbps,
	Przepustowość urządzenia pracującego jako koncentrator VPN: 2,1 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544
	Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – 3,0 Gbps,
	Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 2 000
	Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych.
	Zintegrowany system skanowania antyspyware,
	Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www.
	System IPS musi używać algorytmu szeregowego przetwarzania.

	Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex).
	Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji, a) Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie. b) Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur, Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur
	System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.
	Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa,
	Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi,
	Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p,
	Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń, Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Funkcjonalność nie może wymagać zakupu dodatkowych licencji.
	Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss. Funkcjonalność nie może wymagać zakupu dodatkowych licencji.
	Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 32 takich punktów dostępowych sieci bezprzewodowej.
Połączenia VPN	Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 10 z możliwością rozszerzenia do przynajmniej 500

	Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 50 z możliwością rozszerzenia do przynajmniej 1 000
	Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne
	Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 800 Mbps oraz obsłużyć 125 000 połączeń
	Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP,
	Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site),
Uwierzytelnianie	Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP
	Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa),
Kontrola WWW	Wsparcie dla Dynamicznego DNS tzw. DDNS
	Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne.
	Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio).
	Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak: a) wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron), b) wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony, c) wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki.
	Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii

	Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps,
Bezpieczeństwo	Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci.
	Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL.
	Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty.
Polityki Firewall	Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego
	Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN),
	Kontrola dostępności zestawionych tuneli VPN,
Zarządzanie	Narzędzie działające w trybie multi-tenant, które umożliwia centralne zarządzenia wszystkimi operacjami firewalli
	Narzędzie umożliwiające zatwierdzenia konfiguracji przez inne osoby administracyjne niż te które stworzyły konfigurację IPFIX do zbierania logów
	Narzędzie , które w połączeniu z analityką zapewnia widoczność przez 7 dni w tygodniu całego ekosystemu na poziomie tenantu, grupy lub urządzenia
Gwarancja podstawowa	Min. 24 mc, wsparcie w trybie 24x7.

Licencje – 1 szt.

Kwota jednostkowa netto [PLN]	Kwota jednostkowa brutto [PLN]	Koszt netto [PLN]	Koszt brutto [PLN]

Wymagane licencje	Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 2 lat. 10 użytkowników dla połączeń SSL VPN

Usługa uruchomienia i konfiguracji Firewall – 1 szt.

Kwota jednostkowa netto [PLN]	Kwota jednostkowa brutto [PLN]	Koszt netto [PLN]	Koszt brutto [PLN]

Zakres prac Firewall	Instalacja urządzeń w wskazanych lokalizacjach oddalonych od siebie maksymalnie o 4 km. Rejestracja urządzeń na portalu klienta. Konfiguracja serwera czasu i strefy czasowej Wskazanie lokalizacji przetwarzania danych zaawansowanej ochrony przed zagrożeniami. Uruchomienie: • Adresacji sieci WAN

	• Adresacji sieci LAN + 5 Vlanów • Adresacji sieci do zarządzania infrastrukturą IT. • Połączenia VPN pomiędzy oddziałami z możliwością stosowania polityk firewall. • Integracji z Active Directory • Polityk działających na podstawie grup AD. Stworzenie kopii zapasowej i przywracanie do pracy urządzenia po skasowaniu konfiguracji. Szkolenie z zarządzania regułami i przywracania środowiska po awarii.

Firewall - 1 szt.			
Kwota jednostkowa netto [PLN]	Kwota jednostkowa brutto [PLN]	Koszt netto [PLN]	Koszt brutto [PLN]

Komponent	**Minimalne wymagania**
Wymagania ogólne	Zapora sieciowa typu Next Generation Firewall (NGFW)
	Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku
	Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić)
	Funkcja NAT oparta o reguły bezpieczeństwa
	NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe)
	System musi pochodzić z oficjalnej dystrybucji producenta
	Urządzenie powinno mieć możliwość mocowania w szafie Rack
Ilość urządzeń	1 sztuka
Interfejsy sieciowe Wbudowane i dodatkowe	2 interfejsów 2.5 GbE SFP+,
	8 interfejsy RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa.
	2 interfejsy USB 3.0 dla przyszłych potrzeb i do podłączenia modemu 3G,
	1 interfejs konsoli do zarządzania zaporą,
	1 interfejs RJ-45 Ethernet 10/100/1000 do zarządzania zaporą

	Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa
	Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji
	Możliwość utworzenia przynajmniej 256 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q
	Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej
Dysk	Zapora powinna posiadać możliwość montażu dysku o pojemności przynajmniej 256 GB
Parametry Wydajnościowe	Minimalna ilość jednocześnie obsługiwanych połączeń: 1 250 000,
	Możliwość obsłużenia przynajmniej 16 000 nowych połączeń w ciągu 1 sekundy.
	Przepustowość urządzenia pracującego w trybie stateful firewall: 4 Gbps – dla ramki 1518B zgodnie z RFC 2544
	Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 2,5 Gbps,
	Przepustowość urządzenia pracującego jako koncentrator VPN: 1,8 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544,
	Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – 2,0 Gbps,
	Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 200
	Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych.
	Zintegrowany system skanowania antyspyware,
	Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www.

	System IPS musi używać algorytmu szeregowego przetwarzania.
	Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex).
	Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji, a) Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie. b)Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur, c) Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur
	System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.
	Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa,
	Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi,
	Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p,
	Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń
	Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Funkcjonalność nie może wymagać zakupu dodatkowych licencji.
	Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss. Funkcjonalność nie może wymagać zakupu dodatkowych licencji.
	Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 32 takich punktów dostępowych sieci bezprzewodowej.

Połączenia VPN	Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 10 z możliwością rozszerzenia do przynajmniej 200
	Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 50 z możliwością rozszerzenia do przynajmniej 500
	Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne
	Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 750 Mbps oraz obsłużyć 5 000 połączeń
	Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP,
	Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site),
Uwierzytelnianie	Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP
	Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa),
Kontrola WWW	Wsparcie dla Dynamicznego DNS tzw. DDNS
	Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne.
	Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio).
	Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak: a) wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron), b) wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony, c) wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej

	kategorii. Użytkownik może wejść na stronę po akceptacji polityki.
	Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps,
Bezpieczeństwo	Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci.
	Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL.
	Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty.
Polityki Firewall	Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego
	Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN),
	Kontrola dostępności zestawionych tuneli VPN,
Zarządzanie	Narzędzie działające w trybie multi-tenant, które umożliwia centralne zarządzenia wszystkimi operacjami firewalli
	Narzędzie umożliwiające zatwierdzenia konfiguracji przez inne osoby administracyjne niż te które stworzyły konfigurację IPFIX do zbierania logów
	Narzędzie , które w połączeniu z analityką zapewnia widoczność przez 7 dni w tygodniu całego ekosystemu na poziomie tenantu, grupy lub urządzenia

Gwarancja podstawowa	Min. 24 mc, wsparcie w trybie 24x7.
Wymagane licencje	Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 2 lat.

Licencje – 1 szt.

Kwota jednostkowa netto [PLN]	Kwota jednostkowa brutto [PLN]	Koszt netto [PLN]	Koszt brutto [PLN]

Wymagane licencje	Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 2 lat.

Usługa uruchomienia i konfiguracji Firewall – 1 szt.			
Kwota jednostkowa netto [PLN]	Kwota jednostkowa brutto [PLN]	Koszt netto [PLN]	Koszt brutto [PLN]

Zakres prac Firewall	Instalacja urządzeń w wskazanych lokalizacjach oddalonych od siebie maksymalnie o 4 km. Rejestracja urządzeń na portalu klienta. Konfiguracja serwera czasu i strefy czasowej Wskazanie lokalizacji przetwarzania danych zaawansowanej ochrony przed zagrożeniami. Uruchomienie: ● Adresacji sieci WAN ● Adresacji sieci LAN + 5 Vlanów ● Adresacji sieci do zarządzania infrastrukturą IT. ● Połączenia VPN pomiędzy oddziałami z możliwością stosowania polityk firewall. ● Integracji z Active Directory ● Polityk działających na podstawie grup AD. Stworzenie kopii zapasowej i przywracanie do pracy urządzenia po skasowaniu konfiguracji. Szkolenie z zarządzania regułami i przywracania środowiska po awarii.