Załącznik nr 1 do SIWZ

wzór

OFERTA

(formularz ofertowy)

Nazwa i adres Wykonawcy:

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

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

NIP .................................................... REGON ...........................................................................

Adres, na który Zamawiający powinien przesyłać ewentualną korespondencję:

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

Osoba wyznaczona do kontaktów z Zamawiającym:

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

Numer telefonu:.............................................

Numer faksu...................................................

e-mail .............................................................

W odpowiedzi na ogłoszenie o przetargu nieograniczonym składamy niniejszą ofertę   
w postępowaniu pn: **„Odnowienie subskrypcji oprogramowania/ wsparcia wraz   
z wyrównaniem terminu do 15.02.2018 r. dla urządzeń typu UTM, AP, analizujących ruch sieciowy, monitorujących ruch www i zabezpieczających serwery poczty elektronicznej używanych przez Zamawiającego”** – znak sprawy nr 24/ ZP/ 2016 **oferując wykonanie przedmiotu zamówienia za łączną CENĘ OFERTOWĄ:**

CENA OFERTY NETTO………………………………………………………zł

(słownie ……………………………………………………………………..……............................zł)

plus podatek VAT (23%) w kwocie …………………………………………….. zł.

CENA OFERTY BRUTTO………………………………………………………zł

(słownie ……………………………………………………………………..……............................zł)

Obliczoną zgodnie z poniższą kalkulacją:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***Lp.*** | ***Aktualizacja dla produktu*** | ***Oferowane urządzenie  (nazwa, producent, model, rok produkcji)***  ***- w przypadku gdy Wykonawca oferuje rozwiązanie równoważne*** | ***j.m.*** | ***Ilość*** | ***Cena jednostkowa netto*** | ***Cena*** | ***Wartość brutto*** |
| ***jednostkowa brutto*** |
| ***1*** | ***2*** | ***3*** | ***4*** | ***5*** | ***6*** | ***7*** | ***8 (5 x 7)*** |
| ***1.*** | *Pakiet licencji dla FortiAP 220B* |  | ***szt.*** | ***1*** |  |  |  |
| ***2.*** | *Pakiet licencji dla FortiMail 100C* |  | ***szt.*** | ***1*** |  |  |  |
| ***3.*** | *Pakiet licencji dla FortiGate 200B* |  | ***szt.*** | ***2*** |  |  |  |
| ***4.*** | *Pakiet licencji dla FortiGate 40C* |  | ***szt.*** | ***23*** |  |  |  |
| ***5.*** | *Pakiet licencji dla FortiGate 60C* |  | ***szt.*** | ***1*** |  |  |  |
| ***6.*** | *Pakiet licencji dla FortiAnalyzer 100C* |  | ***szt.*** | ***1*** |  |  |  |
| ***7.*** | *Pakiet licencji dla FortiManager -VM* |  | ***szt.*** | ***1*** |  |  |  |
| ***8.*** | *Pakiet licencji dla FortiAP 223B* |  | ***szt.*** | ***48*** |  |  |  |
| ***9.*** | *Pakiet licencji dla FortiWeb 400C* |  | ***szt.*** | ***1*** |  |  |  |
| ***10.*** | *Pakiet licencji dla FortiGate 800C od 19.11.2017 r. do 15.02.2018 r.* |  | ***szt.*** | ***2*** |  |  |  |
|  | ***Razem*** | | | | | |  |

* + 1. **OŚWIADCZAMY,** że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia iuznajemy się za związanych określonymi w niej postanowieniami i zasadami postępowania.
    2. **ZOBOWIĄZUJEMY SIĘ** do wykonania zamówienia w terminie określonym w Rozdziale V SIWZ.

3. **AKCEPTUJEMY** warunki płatności określone przez Zamawiającego we  wzorze Umowy (minimalny termin płatności: 14 dni od otrzymania faktury przez Zamawiającego).

4**. UWAŻAMY SIĘ** za związanych niniejszą ofertą przez czas wskazany w Specyfikacji Istotnych Warunków Zamówienia, tj. przez okres 30 dni uwzględniając, że termin składania ofert jest pierwszym dniem biegu terminu.

5. **OŚWIADCZAMY,** że termin dostawy produktów wynosi ………. dni.

Uwaga: maksymalny termin dostawy produktów wynosi 30 dni. W przypadku zaoferowania rozwiązań równoważnych termin ten obejmuje dostawę sprzętu, oprogramowania, licencji, wdrożenia   
i instalację sprzętu wraz z oprogramowaniem, przeprowadzenie testów oraz przeszkolenie personelu Zamawiającego.

6. **PRZYJMUJEMY** do wiadomości[[1]](#footnote-1), że niewypełnienie pozycji określonych w kolumnie „dane techniczne oferowanego sprzętu” w tabeli Załącznika nr 1 A do SIWZ „Wymagane minimalne parametry techniczne” w sposób wymagany lub udzielenie odpowiedzi negatywnej ,,nie spełnia’’ spowoduje odrzucenie oferty, o ile z treści innych dokumentów stanowiących załączniki do oferty nie będzie wynikało, iż oferowane urządzenia spełniają wymagania określone w ww. tabeli.

7. OŚWIADCZAMY, że *(\*niepotrzebne skreślić, a wymagane informacje uzupełnić, jeśli   
 dotyczy*):

- nie zamierzamy powierzać wykonania części zamówienia podwykonawcom

- zamierzamy powierzyć wykonanie następujących części zamówienia niżej wymienionym podwykonawcom: ……………………………………………………………………………………………………………………………………………………

Zgodnie z Rozdziałem VII ust. 10 SIWZ wskazuję dostępność poniżej wskazanych oświadczeń lub dokumentów, o których mowa w Rozdziale VII ust. 5 SIWZ w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych (jeżeli dotyczy):

|  |  |
| --- | --- |
| Nazwa oświadczenia lub dokumentu (lub odpowiednie odesłanie do dokumentu wymaganego w SIWZ np. Rozdział VII ust. 5 pkt … SIWZ ): | Adres strony internetowej ogólnodostępnej i bezpłatnej bazy danych |
|  |  |
|  |  |
|  |  |

Oferta została złożona na ……. parafowanych i kolejno ponumerowanych stronach.

Do oferty dołączono następujące załączniki:

Załącznik nr 1 – Oświadczenie dotyczące spełniania warunków

Załącznik nr 2 – Oświadczenie dotyczące przesłanek wykluczenia z postępowania

………………..............................................................

(data, imię i nazwisko oraz podpis upoważnionego przedstawiciela Wykonawcy)

Załącznik nr 2 do SIWZ

**Zamawiający:**

**Polska Akademia Nauk**

Plac Defilad 1, 00-901 Warszawa

www.pan.pl

NIP: 5251575083, REGON: 000325713

Tel.: (22) 826 37 76, Faks: (22) 826 65 12

**Wykonawca:**

………………………………………………………………………………

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

reprezentowany przez:

………………………………………………………………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

**Oświadczenie wykonawcy**

**składane na podstawie art. 25a ust. 1 ustawy z dnia 29 stycznia 2004 r.**

**Prawo zamówień publicznych (dalej jako: ustawa Pzp),**

**DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Odnowienie subskrypcji oprogramowania/ wsparcia wraz z wyrównaniem terminu do 15.02.2018 r. dla urządzeń typu UTM, AP, analizujących ruch sieciowy, monitorujących ruch www   
i zabezpieczających serwery poczty elektronicznej używanych przez Zamawiającego”** – znak sprawy nr 24/ ZP/ 2016 oświadczam co następuje:

**OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:**

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie   
   art. 24 ust 1 pkt 12-23 ustawy Pzp.
2. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie   
   art. 24 ust. 5 ustawy Pzp .

…………….……. *(miejscowość),* dnia ………….……. r.

…………………………………………

*(podpis)*

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. …………. ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 24 ust. 1 pkt 13-14, 16-20 lub art. 24 ust. 5 ustawy Pzp).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 24 ust. 8 ustawy Pzp podjąłem następujące środki naprawcze:

……………………………………………………………………………………………………………………..

…………………………………………………………………………………………..…………………...........………………………………………………………………………………………………………………………………………………………………………………………………………………………………………….………

…………….……. *(miejscowość),* dnia …………………. r.

…………………………………………

*(podpis)*

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

Oświadczam, że następujący/e podmiot/y, 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 podlega/ją wykluczeniu z postępowania o udzielenie zamówienia.

…………….……. *(miejscowość),* dnia …………………. r.

…………………………………………

*(podpis)*

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

Oświadczam, że następujący/e podmiot/y, będący/e podwykonawcą/ami:

……………………………………………………………………………………………………..………..….…… *(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*, nie podlega/ą wykluczeniu z postępowania o udzielenie zamówienia.

…………….……. *(miejscowość),* dnia …………………. r.

…………………………………………

*(podpis)*

**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),* dnia …………………. r.

…………………………………………

*(podpis)*

Załącznik nr 3 do SIWZ

**Zamawiający:**

**Polska Akademia Nauk**

Plac Defilad 1, 00-901 Warszawa

www.pan.pl

NIP: 5251575083, REGON: 000325713

Tel.: (22) 826 37 76, Faks: (22) 826 65 12

**Wykonawca:**

………………………………………………………………………………

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

reprezentowany przez:

………………………………………………………………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

**Oświadczenie wykonawcy**

**składane na podstawie art. 25a ust. 1 ustawy z dnia 29 stycznia 2004 r.**

**Prawo zamówień publicznych (dalej jako: ustawa Pzp),**

**DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Odnowienie subskrypcji oprogramowania/ wsparcia wraz z wyrównaniem terminu do 15.02.2018 r. dla urządzeń typu UTM, AP, analizujących ruch sieciowy, monitorujących ruch www   
i zabezpieczających serwery poczty elektronicznej używanych przez Zamawiającego”**– znak sprawy nr 24/ ZP/ 2016 oświadczam co następuje:

**INFORMACJA DOTYCZĄCA WYKONAWCY:**

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez zamawiającego w      …………..…………………………………………………..……………………………………………….. *(wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu)*.

…………….……. *(miejscowość),* dnia ………….……. r.

…………………………………………

*(podpis)*

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

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w ………………………………………………………...…………………………….. *(wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu),* polegam na zasobach następującego/ych podmiotu/ów:

……………………………………………………………………………………………………………………….

..……………………………………………………………………………………………………………….……..w następującym zakresie: …………………………………………………………………………………...…

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

…………….……. *(miejscowość),* dnia ………….……. r.

…………………………………………

*(podpis)*

**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),* dnia ………….……. r.

…………………………………………

*(podpis)*

Załącznik nr 4 do SIWZ

**Zamawiający:**

**Polska Akademia Nauk**

Plac Defilad 1, 00-901 Warszawa

www.pan.pl

NIP: 5251575083, REGON: 000325713

Tel.: (22) 826 37 76, Faks: (22) 826 65 12

**Wykonawca:**

………………………………………………………………………………

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

reprezentowany przez:

………………………………………………………………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

OŚWIADCZENIE

DOTYCZĄCE PRZYNALEŻNOŚCI DO GRUPY KAPITAŁOWEJ

W związku z ubieganiem się o udzielenie zamówienia publicznego pn. **„Odnowienie subskrypcji oprogramowania/ wsparcia wraz z wyrównaniem terminu do 15.02.2018 r. dla urządzeń typu UTM, AP, analizujących ruch sieciowy, monitorujących ruch www   
i zabezpieczających serwery poczty elektronicznej używanych przez Zamawiającego”**– znak sprawy nr 24/ ZP/ 2016 oświadczam/my, że:

1. należę/my do tej samej grupy kapitałowej (w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. 2015 r., poz. 184 z późn. zm.), wraz z następującymi wykonawcami, którzy złożyli odrębne oferty:\*
2. ………………………………………………………………...……………………………………..
3. …………………………………………………………………………………………...…………..
4. ……………………………………………………………………………………………………….
5. nie należę/my do grupy kapitałowej, wraz z innymi wykonawcami, którzy złoży odrębne oferty\*

# \* niepotrzebne skreślić

Uwaga: w przypadku przynależności do tej samej grupy kapitałowej wykonawca może złożyć, wraz z oświadczeniem dokumenty bądź informacje potwierdzające, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu.

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

data imię i nazwisko podpis wykonawcy lub osoby   
 upoważnionej

Załącznik nr 5a do SIWZ

**Wymagania dla rozwiązania równoważnego**

1. FortiAP 220B 1szt

Wymagane parametry równoważności:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | | **Dane techniczne oferowanego sprzętu**  *(\*niepotrzebne skreślić,  a wymagane pola uzupełnić)* |
| **Oferowane urządzenia:**  **Producent: …………………………………………………………………………**  **Model: ………………………………………………………………………………**  **Rok produkcji: …………………………………………………………………**  (**\****należy uzupełnić wszystkie wykropkowane pola)* | | |  |
|  | | | |
|  | Tryb pracy | Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. Ze względu na instniejącą infrastrukturę i uzyskania wymaganego poziomu bezpieczeństwa kontroler sieci wireless ma być uruchomiony w obrębie urządzenia bezpieczeństwa gwarantującego ochronę dla obsługiwanych sieci wireless i przewodowych. W posiadaniu Zamawiającego jest urządzenie klasy UTM – Fortigate 800C. | **Spełnia/Nie spełnia**\* |
|  | Moduł radiowy | Musi być wyposażone w dwa niezależne moduły radiowe, jeden z nich ma pracować w paśmie 5 GHz a/n lub 2,4 GHz b/g/n (do wyboru), drugi natomiast ma zapewniać obsługę zakresu 2,4 GHz b/g/n.  Musi pozwalać na jednoczesne rozgłaszanie co najmniej 14 SSID.  Wymagana moc nadawania min 17dBm. | *Ilość niezależnych modułów radiowych:*  *……………………………….*  *Ilość jednocześnie rozgłaszanych SSID:*  *……………………………….*  *Moc nadawania:*  *……………………………….*  **Spełnia/Nie spełnia**\* |
|  | Anteny | Minimum 2 anteny wbudowane | *Ilość wbudowanych anten:*  *……………………………….*  **Spełnia/Nie spełnia**\* |
|  | Interfejsy | Minimum 1 interfejs w standardzie 10/100/1000 Base-TX | *Ilość interfejsów w standardzie 10/100/1000 Base-TX:*  *……………………………….*  **Spełnia/Nie spełnia**\* |
|  | Zasilanie | Możliwość zasilania w standardzie PoE 802.3af | **Spełnia/Nie spełnia**\* |
|  | Oprogramowanie | Możliwosć aktualizacji firmware minimum przez 12 miesięcy | **Spełnia/Nie spełnia**\* |

1. FortiMail 100C 1szt

Wymagane parametry równoważności:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | | **Dane techniczne oferowanego sprzętu** |
| *(\*niepotrzebne skreślić,  a wymagane pola uzupełnić)* |
| **Oferowane urządzenia:** | | |  |
| **Producent:……………………………………………………………………….** | | |
| **Model…………………………………………………………………………….** | | |
| **Rok produkcji: ………………………………………………………………..**  (**\****należy uzupełnić wszystkie wykropkowane pola)* | | |
|  | | | |
| 1. | System | Opcje instalacji w trybie transparentnym, bramki i serwera |  |
|  |
|  |
| Obsługa VLAN i interfejsów redundantnych |  |
| Obsługa adresów IPv6 i IPv4 |  |
| Wirtualny hosting korzystający z zasobów źródłowych i/lub docelowych adresów IP |  |
| Obsługa uwierzytelnienia SMTP za pośrednictwem serwerów LDAP, RADIUS,POP3 i IMAP |  |
| Routnig wiadomości e-mail z użyciem protokołu LDAP |  |
| Kompleksowy interfejs WebMail do operacji w trybie serwera i zarządzania kwarantanną | **Spełnia/Nie spełnia**\* |
| Zarządzanie kolejką wiadomości |  |
| Kontrola każdego z użytkowników na podstawie reguł dla danej domeny z użyciem atrybutów LDAP |  |
| Uwierzytelnianie wiadomości e-mail |  |
| Tworzenie lokalnej listy reputacji nadawców na podstawie metod sender policy framework, domain keys Identified Mail |  |
| Kontrola wiadomości przychodzących i wychodzących |  |
| Wiele domen poczty elektronicznej z możliwością konfiguracji hierarchicznej |  |
| Kompletna, wielowarstwowa ochrona antywirusowa, antyspamowa, przeciw złośliwemu oprogramowaniu i atakom typu fishing dla nieograniczonej liczby użytkowników. |  |
| 2. | Zarządzanie , rejestrowanie, raportowanie | Konta administracyjne dla każdej z domen oparte na rolach |  |
| Kompleksowe rejestrowanie i raportowanie aktywności i incydentów |  |
| Rejestr zmian konfiguracji i zdarzeń dotyczących zarządzania |  |
| Wbudowany moduł raportujący |  |
| Wsparcie ze strony rozwiązań **służących do centralnego zarządzania i raportowania opisanych w punktach F i G** | **Spełnia/Nie spełnia**\* |
| Obsługa protokołu SNMP z użyciem standardowych i personalizowanych plików MIB |  |
| Obsługa zewnętrznych lub lokalnych zasobów pamięci masowej , w tym urządzeń iSCSI |  |
| Obsługa zewnętrznych zdarzeń |  |
| 3. | Wydajnosć | tryb Acticve-Passive |  |
| Synchronizacja kwarantanny i kolejek wiadomości | **Spełnia/Nie spełnia**\* |
| Wykrywanie usterek urządzneiea i powiadamianie o nich |  |
| Monitorowanie statusu łącza, przełączeń awaryjnych wraz z obsługą interfejsu nadmiarowego |  |
| 4. | Szyfrowanie | Szyfrowanie na podstawie tożsamości w przesyle wiadomosci w trybie Push i Pull |  |
| Obsługa standardu S/MIME w szyfrowaniu miedzy serwerami pocztowymi | **Spełnia/Nie spełnia**\* |
| Obsługa silnych protokołów szfrujących , w tym HTTPS,SMTPS,SSH,IMAPS i POP3S |  |
| 5. | tryb serwera | Usługi poczty e-mail SMTP,IMAP,POP3 |  |
| Obsługa protokołu SMTP over SSl |  |
| Obsługa polityk przydziału przestrzeni dyskowej dla użytkowników |  |
| Bezpieczny dostęp do klienta Webmail | **Spełnia/Nie spełnia**\* |
| Obsługa list użytkowników, grp i pseudonimów |  |
| Uwierzytelnianie konta na poziomie lokalnym i serwera LDAP |  |
| Kalendarz WebMail |  |
| Preferencje dotyczące automatycznego odpowiadamia i przesyłania wiadomości dalej |  |
| Synchronizacja ksiązki adresowej z sererem LDAP |  |
| 6. | Oprogramowanie | oprogramowanie typu antywirus, antyspam licencja minimum na 12 miesięcy  Możliwosć aktualizacji firmware minimum przez 12 miesięcy | **Spełnia/Nie spełnia**\* |

1. FortiGate 200B 2 szt

Wymagane parametry równoważności:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | | | **Dane techniczne oferowanego sprzętu**  *(\*niepotrzebne skreślić, a wymagane pola uzupełnić)* |
| **Oferowane urządzenia:**  **Producent:………………………………………………………………………. Model…………………………………………………………………………….**  **Rok produkcji: ………………………………………………………………….**  (**\****należy uzupełnić wszystkie wykropkowane pola)* | | | |  |
|  | |  | |  |
|  | | Architektura systemu ochrony | Główne urządzenie ochronne [gateway] musi używać pamięć FLASH. (nie dopuszcza się użycia dysku)  Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanego układu ASIC.  Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie). | **Spełnia/Nie spełnia**\* |
|  | | System operacyjny | Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia. | **Spełnia/Nie spełnia**\* |
|  | | Ilość/rodzaj portów | Nie mniej niż **8** portów Ethernet 10/100/1000 Base-TX.  Nie mniej niż **4080** interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard IEEE802.1q | *Liczba portów*  Ethernet 10/100/1000 BASE-TX*..........*  *Liczba interfejsów wirtualnych…………..*  **Spełnia/Nie spełnia**\* |
|  | | Funkcjonalności podstawowe i uzupełniające | System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych:  - kontrolę dostępu - zaporę ogniową klasy Stateful Inspection  - ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP). Kontrola AV powinna bazować na analizie plików z wykorzystaniem technologii proxy.  - poufność danych - IPSec VPN oraz SSL VPN  - ochronę przed atakami - Intrusion Prevention System [IPS/IDS]  - oraz funkcjonalności uzupełniających:  - kontrolę treści – Web Filter [WF]  - kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP; POP3, IMAP)   * kontrolę pasma oraz ruchu [QoS i Traffic shaping] * kontrolę aplikacji (minimum IM oraz P2P) | **Spełnia/Nie spełnia**\* |
|  | | Zasada działania (tryby) | Urządzenie musi dawać możliwość ustawienia jednego z dwóch trybów pracy:  - jako router/NAT (3.warstwa ISO-OSI) lub  - jako most /transparent bridge/ . Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu. | **Spełnia/Nie spełnia**\* |
|  | | Polityka bezpieczeństwa (firewall) | Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników sieci, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem (m.in. pasmo gwarantowane i maksymalne, priorytety). | **Spełnia/Nie spełnia**\* |
|  | | Wykrywanie ataków | Wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP.   * Nie mniej niż 4000 sygnatur ataków. * Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie * Możliwość wykrywania anomalii protokołów i ruchu | **Spełnia/Nie spełnia**\* |
|  | | Translacja adresów | Statyczna i dynamiczna translacja adresów (NAT).  Translacja NAPT. | **Spełnia/Nie spełnia**\* |
|  | | Wirtualizacja i routing dynamiczny | Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne ustawienia wszystkich funkcji bezpieczeństwa i dostęp administracyjny.  Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego.  Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM. | **Spełnia/Nie spełnia**\* |
|  | | Połączenia VPN | Wymagane nie mniej niż:  - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site  - Dostawca musi udostępniać klienta VPN własnej produkcji  - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności  - Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN)  - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth | **Spełnia/Nie spełnia**\* |
| 1. 11 | | Uwierzytelnianie użytkowników | System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:  -haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia  -haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP  - haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych  Rozwiązanie musi umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych. | **Spełnia/Nie spełnia**\* |
|  | | Wydajność | Obsługa nie mniej niż **500 tys** jednoczesnych połączeń i **15 tys** nowych połączeń na sekundę  Przepływność nie mniejsza niż **5 Gbps** dla ruchu nieszyfrowanego i **1,5 Gbps** dla VPN (3DES).  Obsługa nie mniej niż **2000** jednoczesnych tuneli VPN | *Liczba jednoczesnych połączeń………*  *Liczba nowych połączeń……..*  *Przepływność Gbps dla ruchu nie szyfrowanego………*  *Przepływność Gpps dla VPN (3DES)………*  *Liczba jednoczesnych tuneli VPN………*  **Spełnia/Nie spełnia**\* |
|  | | Funkcjonalność zapewniająca niezawodność | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive.  System powinien zostać dostarczony w formie klastra urządzeń. | **Spełnia/Nie spełnia**\* |
|  | | Konfiguracja i zarządzanie | Możliwość konfiguracji poprzez terminal i linię komend oraz wbudowaną konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą:   * haseł statycznych * haseł dynamicznych (RADIUS, RSA SecureID)   System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB.  Jednocześnie, dla systemu bezpieczeństwa powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta. | **Spełnia/Nie spełnia**\* |
|  | | Zarządzanie | System musi mieć możliwość współpracy z zewnętrznym, sprzętowym modułem centralnego zarządzania umożliwiającym:   * Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej * Wersjonowanie polityk w taki sposób aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości * Zarządzanie wersjami firmware’u na urządzeniach oraz zdalne uaktualnienia * Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia * Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM) * Zapis i zdalne wykonywanie skryptów na urządzeniach | **Spełnia/Nie spełnia**\* |
|  | | Raportowanie | System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym:   * Zbieranie logów z urządzeń bezpieczeństwa * Generowanie raportów * Skanowanie podatności stacji w sieci * Zdalną kwarantannę dla modułu antywirusowego   System musi posiadać również funkcję lokalnego logowania i przechowywania logów o sumarycznym rozmiarze min. 63GB. | *……….sumaryczna wielkość logów*  **Spełnia/Nie spełnia**\* |
|  | | Integracja systemu zarządzania | Zgodnie z zaleceniami normy PN-ISO/17799 zarówno moduł centralnego zarządzania jak i raportowania muszą być zrealizowane na osobnych urządzeniach sprzętowych. Jednocześnie administrator powinien mieć do dyspozycji jedną konsolę zarządzającą do kontroli obu podsystemów. | **Spełnia/Nie spełnia**\* |
| 1. 1. | | Oprogramowanie | oprogramowanie typu antywirus, antyspam, IPS, Web Filter licencja minimum na 12 miesięcy  Możliwosć aktualizacji firmware przez minimum na 12 miesięcy | **Spełnia/Nie spełnia**\* |

1. FortiGate 40C 23 szt

Wymagane parametry równoważności:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | | **Dane techniczne oferowanego sprzętu**  *(należy uzupełnić wszystkie wykropkowane pola)*  *(\*niepotrzebne skreślić, a wymagane pola uzupełnić)* |
| **Oferowane urządzenia:**  **Producent: ………………………………………………………………………**  **Model: ……………………………………………………………………………**  **Rok produkcji: …………………………………………………………………**  (**\****należy uzupełnić wszystkie wykropkowane pola)* | | |  |
|  |  | |  |
| 1. | Architektura systemu ochrony | Główne urządzenie ochronne [gateway] musi używać pamięć FLASH. (nie dopuszcza się użycia dysku)  Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanego układu ASIC.  Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie). | **Spełnia/Nie spełnia**\* |
| 2. | System operacyjny | Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia. | **Spełnia/Nie spełnia**\* |
| 3. | Ilość/rodzaj portów | Nie mniej niż 2 porty WAN Ethernet Interfaces 10/100 Base-TX.  Nie mniej niż 1 port DMZ Ethernet 10/100 Base-TX  Nie mniej niż 5portów Ethernet 10/100/1000 Base-TX.  Nie mniej niż 256interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard IEEE802.1q  Urządzenie musi posiadać SD slot 1 szt. | *Liczba portów WAN* Ethernet Interfaces 10/100 BASE-TX*..........*  *Liczba portów* DMZ Ethernet 10/100 BASE-TX*……….......*  *Liczba portów* Ethernet  10/100/1000 BASE-X*……….......*  *Liczba interfejsów wirtualnych…………..*  *Licbaz slotów SD……….*  **Spełnia/Nie spełnia**\* |
| 4. | Funkcjonalności podstawowe i uzupełniające | System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych:   * kontrolę dostępu - zaporę ogniową klasy Stateful Inspection * ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP). Kontrola AV powinna bazować na analizie plików z wykorzystaniem technologii proxy. * poufność danych - IPSec VPN oraz SSL VPN * ochronę przed atakami - Intrusion Prevention System [IPS/IDS] * oraz funkcjonalności uzupełniających: * kontrolę treści – Web Filter [WF] * kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP; POP3, IMAP) * kontrolę pasma oraz ruchu [QoS i Traffic shaping] * kontrolę aplikacji (minimum IM oraz P2P) | **Spełnia/Nie spełnia**\* |
| 5. | Zasada działania (tryby) | Urządzenie musi dawać możliwość ustawienia jednego z dwóch trybów pracy:   * jako router/NAT (3.warstwa ISO-OSI) * lub jako most /transparent bridge/ . Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu. | **Spełnia/Nie spełnia**\* |
| 6. | Polityka bezpieczeństwa (firewall) | Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników sieci, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem (m.in. pasmo gwarantowane i maksymalne, priorytety). | **Spełnia/Nie spełnia**\* |
| 7. | Wykrywanie ataków | Wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP.   * Nie mniej niż 4000 sygnatur ataków. * Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie   Możliwość wykrywania anomalii protokołów i ruchu | **Spełnia/Nie spełnia**\* |
| 8. | Translacja adresów | Statyczna i dynamiczna translacja adresów (NAT).  Translacja NAPT. | **Spełnia/Nie spełnia**\* |
| 9. | Wirtualizacja i routing dynamiczny | Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne ustawienia wszystkich funkcji bezpieczeństwa i dostęp administracyjny.  Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego.  Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM. | **Spełnia/Nie spełnia**\* |
| 10. | Połączenia VPN | Wymagane nie mniej niż:   * Tworzenie połączeń w topologii Site-to-site oraz Client-to-site * Dostawca musi udostępniać klienta VPN własnej produkcji * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności * Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN)   Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth | **Spełnia/Nie spełnia**\* |
| 11. | Uwierzytelnianie użytkowników | System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:   * haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia * haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP * haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych   Rozwiązanie musi umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych. | **Spełnia/Nie spełnia**\* |
| 12. | Wydajność | Obsługa nie mniej niż **80 tys** jednoczesnych połączeń i **3 tys** nowych połączeń na sekundę  Przepływność nie mniejsza niż **1 Gbps** dla ruchu nieszyfrowanego i **70 Mbps** dla VPN (3DES).  Obsługa nie mniej niż **500** jednoczesnych tuneli VPN | *Liczba jednoczesnych połączeń………*  *Liczba nowych połączeń……..*  *Przepływność Gbps dla ruchu nie szyfrowanego………*  *Przepływność Mbps dla VPN (3DES)………*  *Liczba jednoczesnych tuneli VPN………*  **Spełnia/Nie spełnia**\* |
| 13. | Funkcjonalność zapewniająca niezawodność | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive. | **Spełnia/Nie spełnia**\* |
| 14. | Konfiguracja i zarządzanie | Możliwość konfiguracji poprzez terminal i linię komend oraz wbudowaną konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą:   * haseł statycznych * haseł dynamicznych (RADIUS, RSA SecureID)   System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB.  Jednocześnie, dla systemu bezpieczeństwa powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta. | **Spełnia/Nie spełnia**\* |
| 15. | Zarządzanie | System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem centralnego zarządzania umożliwiającym:   * Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej * Wersjonowanie polityk w taki sposób aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości * Zarządzanie wersjami firmware’u na urządzeniach oraz zdalne uaktualnienia * Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia * Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM)   Zapis i zdalne wykonywanie skryptów na urządzeniach. | **Spełnia/Nie spełnia**\* |
| 16. | Raportowanie | System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym:   * Zbieranie logów z urządzeń bezpieczeństwa * Generowanie raportów * Skanowanie podatności stacji w sieci * Zdalną kwarantannę dla modułu antywirusowego   System musi posiadać również funkcję lokalnego logowania i przechowywania logów o sumarycznym rozmiarze min. 16GB. | *sumaryczna wielkość logów*  *…………………………………*  **Spełnia/Nie spełnia**\* |
| 17. | Integracja systemu zarządzania | Zgodnie z zaleceniami normy PN-ISO/17799 zarówno moduł centralnego zarządzania jak i raportowania muszą być zrealizowane na osobnych urządzeniach sprzętowych. Jednocześnie administrator powinien mieć do dyspozycji jedną konsolę zarządzającą do kontroli obu podsystemów. | **Spełnia/Nie spełnia**\* |
| 18. | Oprogramowanie | oprogramowanie typu antywirus, antyspam, IPS, Web Filter licencja minimum na 12 miesięcy  Możliwosć aktualizacji firmware minimum przez 12 miesięcy. | **Spełnia/Nie spełnia**\* |

1. FortiGate 60C 1szt

Wymagane parametry równoważności:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | | **Dane techniczne oferowanego sprzętu**  *(\*niepotrzebne skreślić, a wymagane pola uzupełnić)* |
| **Oferowane urządzenia:**  **Producent: ………………………………………………………………………**  **Model: ……………………………………………………………………………**  **Rok produkcji: …………………………………………………………………**  (**\****należy uzupełnić wszystkie wykropkowane pola)* | | |  |
|  |  | |  |
| 1. | Architektura systemu ochrony | Główne urządzenie ochronne [gateway] musi używać pamięć FLASH. (nie dopuszcza się użycia dysku)  Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanego układu ASIC.  Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie). | **Spełnia/Nie spełnia**\* |
| 2. | System operacyjny | Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia. | **Spełnia/Nie spełnia**\* |
| 3. | Ilość/rodzaj portów | Nie mniej niż 2 porty WAN Ethernet Interfaces 10/100 Base-TX.  Nie mniej niż 1 port DMZ Ethernet 10/100 Base-TX  Nie mniej niż 5portów Ethernet 10/100/1000 Base-TX.  Nie mniej niż 256interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard IEEE802.1q  Urządzenie musi posiadać SD slot 1 szt. | *Liczba portów WAN* Ethernet Interfaces 10/100 BASE-TX*..........*  *Liczba portów* DMZ Ethernet 10/100 BASE-TX*……….......*  *Liczba portów* Ethernet  10/100/1000 BASE-X*……….......*  *Liczba interfejsów wirtualnych…………..*  *Liczba slotów SD……….*  **Spełnia/Nie spełnia**\* |
| 4. | Funkcjonalności podstawowe i uzupełniające | System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych:   * kontrolę dostępu - zaporę ogniową klasy Stateful Inspection * ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP). Kontrola AV powinna bazować na analizie plików z wykorzystaniem technologii proxy. * poufność danych - IPSec VPN oraz SSL VPN * ochronę przed atakami - Intrusion Prevention System [IPS/IDS] * oraz funkcjonalności uzupełniających: * kontrolę treści – Web Filter [WF] * kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP; POP3, IMAP) * kontrolę pasma oraz ruchu [QoS i Traffic shaping] * kontrolę aplikacji (minimum IM oraz P2P) | **Spełnia/Nie spełnia**\* |
| 5. | Zasada działania (tryby) | Urządzenie musi dawać możliwość ustawienia jednego z dwóch trybów pracy:   * jako router/NAT (3.warstwa ISO-OSI) * lub jako most /transparent bridge/ . Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu. | **Spełnia/Nie spełnia**\* |
| 6. | Polityka bezpieczeństwa (firewall) | Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników sieci, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem (m.in. pasmo gwarantowane i maksymalne, priorytety). | **Spełnia/Nie spełnia**\* |
| 7. | Wykrywanie ataków | Wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP.   * Nie mniej niż 4000 sygnatur ataków. * Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie   Możliwość wykrywania anomalii protokołów i ruchu | **Spełnia/Nie spełnia**\* |
| 8. | Translacja adresów | Statyczna i dynamiczna translacja adresów (NAT).  Translacja NAPT. | **Spełnia/Nie spełnia**\* |
| 9. | Wirtualizacja i routing dynamiczny | Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne ustawienia wszystkich funkcji bezpieczeństwa i dostęp administracyjny.  Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego.  Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM. | **Spełnia/Nie spełnia**\* |
| 10. | Połączenia VPN | Wymagane nie mniej niż:   * Tworzenie połączeń w topologii Site-to-site oraz Client-to-site * Dostawca musi udostępniać klienta VPN własnej produkcji * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności * Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN)   Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth | **Spełnia/Nie spełnia**\* |
| 11. | Uwierzytelnianie użytkowników | System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:   * haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia * haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP * haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych   Rozwiązanie musi umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych. | **Spełnia/Nie spełnia**\* |
| 12. | Wydajność | Obsługa nie mniej niż **80 tys** jednoczesnych połączeń i **3 tys** nowych połączeń na sekundę  Przepływność nie mniejsza niż **1 Gbps** dla ruchu nieszyfrowanego i **70 Mbps** dla VPN (3DES).  Obsługa nie mniej niż **500** jednoczesnych tuneli VPN | *Liczba jednoczesnych połączeń………*  *Liczba nowych połączeń……..*  *Przepływność Gbps dla ruchu nie szyfrowanego………*  *Przepływność Mbps dla VPN (3DES)………*  *Liczba jednoczesnych tuneli VPN………*  **Spełnia/Nie spełnia**\* |
| 13. | Funkcjonalność zapewniająca niezawodność | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive. | **Spełnia/Nie spełnia**\* |
| 14. | Konfiguracja i zarządzanie | Możliwość konfiguracji poprzez terminal i linię komend oraz wbudowaną konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą:   * haseł statycznych * haseł dynamicznych (RADIUS, RSA SecureID)   System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB.  Jednocześnie, dla systemu bezpieczeństwa powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta. | **Spełnia/Nie spełnia**\* |
| 15. | Zarządzanie | System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem centralnego zarządzania umożliwiającym:   * Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej * Wersjonowanie polityk w taki sposób aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości * Zarządzanie wersjami firmware’u na urządzeniach oraz zdalne uaktualnienia * Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia * Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM)   Zapis i zdalne wykonywanie skryptów na urządzeniach. | **Spełnia/Nie spełnia**\* |
| 16. | Raportowanie | System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym:   * Zbieranie logów z urządzeń bezpieczeństwa * Generowanie raportów * Skanowanie podatności stacji w sieci * Zdalną kwarantannę dla modułu antywirusowego   System musi posiadać również funkcję lokalnego logowania i przechowywania logów o sumarycznym rozmiarze min. 16GB. | *sumaryczna wielkość logów*  *…………………………………*  **Spełnia/Nie spełnia**\* |
| 17. | Integracja systemu zarządzania | Zgodnie z zaleceniami normy PN-ISO/17799 zarówno moduł centralnego zarządzania jak i raportowania muszą być zrealizowane na osobnych urządzeniach sprzętowych. Jednocześnie administrator powinien mieć do dyspozycji jedną konsolę zarządzającą do kontroli obu podsystemów. | **Spełnia/Nie spełnia**\* |
| 18. | Oprogramowanie | oprogramowanie typu antywirus, antyspam, IPS, Web Filter licencja minimum na 12 miesięcy  Możliwosć aktualizacji firmwareprzez minimum na 12 miesięcy | *……………………..*  **Spełnia/Nie spełnia**\* |

1. FortiAnalyzer 100C 1szt

Wymagane parametry równoważności:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | | **Dane techniczne oferowanego sprzętu**  *(\*niepotrzebne skreślić, a wymagane pola uzupełnić)* |
| **Oferowane urządzenia:**  **Producent: ………………………………………………………………………**  **Model: ……………………………………………………………………………**  **Rok produkcji: …………………………………………………………………**  (**\****należy uzupełnić wszystkie wykropkowane pola)* | | |  |
|  |  | |  |
|  |  |  |  |
| 1. | Architektura systemu ochrony | System logowania i raportowania musi stanowić centralne repozytorium danych gromadzonych przez wiele urządzeń oraz aplikacji klienckich z możliwością definiowania własnych raportów na podstawie predefiniowanych wzorców.  Jednocześnie, dla zapewnienia bezpieczeństwa i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie, w tym system operacyjny i sprzęt pochodziły od jednego producenta. | **Spełnia/Nie spełnia**\* |
| 2. | System operacyjny | Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa.  Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia. | **Spełnia/Nie spełnia**\* |
| 3. | Parametry fizyczne systemu | Nie mniej niż 1 port Ethernet 10/100  Nie mniej niż 2 porty Ethernet 10/100/1000  Powierzchnia dyskowa - minimum 1 TB | *Podać liczbę portów*  *Liczba portów* Ethernet 10/100*………..............*  10/100/1000*……….......*  *Wielkość dysku……………*  **Spełnia/Nie spełnia**\* |
| 4. | Funkcjonalności podstawowe i uzupełniające | System musi zapewniać:   * Składowanie oraz archiwizację logów z możliwością ich grupowania w oparciu o urządzenia, użytkowników * Możliwość gromadzenia zawartości przesyłanych za pośrednictwem protokołów Web, FTP; email, IM oraz na ich podstawie analizowania aktywności użytkowników w sieci * Kwarantannę dla współpracujących z nim urządzeń. Kwarantanna obejmuje zainfekowane lub wskazane przez analizę heurystyczną pliki. * Przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących * Wyświetlanie nowych logów w czasie rzeczywistym * Analizowanie ruchu w sieci poprzez nasłuch całej komunikacji w segmencie sieci z możliwością jej zapisu i późniejszej analizy * Analizę podatności stacji w sieci wraz z możliwością raportowania wykrytych luk * Export zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych)   Urządzenie musi realizować funkcje skanowania podatności stacji w sieci. | **Spełnia/Nie spełnia**\* |
| 5. | Parametry wydajnościowe | Urządzenie musi obsługiwać:   * nie mniej niż 100 urządzeń sieciowych i 100 urządzeń klienckich /VPN-client/ | *Liczba urządzeń sieciowych………….*  *Liczba urządzeń klienckich………….*  **Spełnia/Nie spełnia**\* |
| 6. | Zarządzanie | System udostępnia:  Lokalny interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH i konsolę szeregową | **Spełnia/Nie spełnia**\* |
| 7. | Zasilanie | Zasilanie z sieci 230V/50Hz. | **Spełnia/Nie spełnia**\* |
| 8. | Oprogramowanie | Możliwosć aktualizacji firmware przez minimum na 12 miesięcy | **Spełnia/Nie spełnia**\* |

1. FortiManager VM 1szt.

Wymagane parametry równoważności:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | | **Dane techniczne oferowanego sprzętu**  *(\*niepotrzebne skreślić,  a wymagane pola uzupełnić)* |
| **Oferowane urządzenia:**  **Producent: ……………………………………………………………………**  **Model: ………………………………………………………………………..**  **Rok produkcji: ………………………………………………………………**  (**\****należy uzupełnić wszystkie wykropkowane pola)* | | |  |
|  | | | |
| 1, | Tryb pracy | Możliwość obsługi minimum 10 instancji wirtualnych VDOM oraz minimum 50 klientami VPN.  Minimum jeden interfejs sieciowy. | *Ilość instancji wirtualnych*  *………………………………*  *Ilość interfejsów sieciowych*  *……………………………….*  **Spełnia/Nie spełnia**\* |

1. FortiAP 223B 48szt

Wymagane parametry równoważności:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | | **Dane techniczne oferowanego sprzętu**  *(\*niepotrzebne skreślić, a wymagane pola uzupełnić)* |
| **Oferowane urządzenia:**  **Producent: ……………………………………………………………………**  **Model: ………………………………………………………………………..**  **Rok produkcji: ………………………………………………………………**  (**\****należy uzupełnić wszystkie wykropkowane pola)* | | |  |
|  | | | |
| 1. | Tryb pracy | Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. Ze względu na instniejącą infrastrukturę i uzyskania wymaganego poziomu bezpieczeństwa kontroler sieci wireless ma być uruchomiony w obrębie urządzenia bezpieczeństwa gwarantującego ochronę dla obsługiwanych sieci wireless i przewodowych. W posiadaniu Zamawiającego jest urządzenie klasy UTM – Fortigate 800C. | **Spełnia/Nie spełnia**\* |
| 2. | Obudowa | Kompaktowa obudowa z tworzywa sztucznego (o max średnicy lub przekątnej 18cm i grubości max 4 cm) umożliwiającą montaż na suficie lub ścianie wewnątrz budynku. Wymaga się aby interfejs sieciowy i inne gniazda - jeśli występują-zlokalizowane były na ściance od strony montażowej urządzenia. | *Wymiary obudowy:*  *……………………………….*  **Spełnia/Nie spełnia**\* |
| 3. | Moduł radiowy | Musi być wyposażone w dwa niezależne moduły radiowe, jeden z nich ma pracować w paśmie 5 GHz a/n lub 2,4 GHz b/g/n (do wyboru), drugi natomiast ma zapewniać obsługę zakresu 2,4 GHz b/g/n.  Musi pozwalać na jednoczesne rozgłaszanie co najmniej 14 SSID.  Wymagana moc nadawania min 17dBm. | *Ilość niezależnych modułów radiowych:*  *……………………………….*  *Ilość jednocześnie rozgłaszanych SSID:*  *……………………………….*  *Moc nadawania:*  *……………………………….*  **Spełnia/Nie spełnia**\* |
| 4. | Anteny | Minimum 4 anteny wbudowane | *Ilość wbudowanych anten:*  *……………………………….*  **Spełnia/Nie spełnia**\* |
| 5. | Interfejsy | Minimum 1 interfejs w standardzie 10/100/1000 Base-TX | *Ilość interfejsów w standardzie 10/100/1000 Base-TX:*  *……………………………….*  **Spełnia/Nie spełnia**\* |
| 6. | Zasilanie | Możliwość zasilania w standardzie PoE 802.3af | **Spełnia/Nie spełnia**\* |
|  | Oprogramowanie | Możliwosć aktualizacji firmware przez minimum na 12 miesięcy | **Spełnia/Nie spełnia**\* |

1. FortiWeb 400C 1szt

Wymagane parametry równoważności:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | | **Dane techniczne oferowanego sprzętu**  *(\*niepotrzebne skreślić, a wymagane pola uzupełnić)* |
| **Oferowane urządzenia:**  **Producent: ……………………………………………………………………**  **Model: ………………………………………………………………………..**  **Rok produkcji: ………………………………………………………………**  (**\****należy uzupełnić wszystkie wykropkowane pola)* | | |  |
|  | | | |
| 1. | Architektura systemu | System ochrony aplikacji webowych oraz Firewall XML - którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń.  System powinien umożliwiać lokalne logowanie oraz raportowanie w oparciu o zestaw predefiniowanych wzorców raportów. Powinna istnieć możliwość implementacji systemu inline w trybach Reverse Proxy lub Transparentnym, jak również implementacji w trybie nasłuchu. | **Spełnia/Nie spełnia**\* |
| 2. | System operacyjny | Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. | **Spełnia/Nie spełnia**\* |
| 3. | Parametry fizyczne systemu | Nie mniej niż 4 porty Ethernet 10/100/1000 Base-T Powierzchnia dyskowa - minimum 1 TB W celu zwiększenia niezawodności system powinien mieć możliwość pracy w konfiguracji HA (High Availability)z trybem Active-Passive  Obudowa urządzenia o wysokości do 1U przystosowana do montażu w standardowej szafie teletechnicznej 19 cali (urządzenie musi zostać dostarczone z kompletem akcesoriów umożliwiających montaż w szafie *19")* | *Ilość portów 10/100/Base T :*  *……………………………….*  *Powierzchnia dyskowa:*  *……………………………….*  *Wysokość obudowy*  *……………………………….*  **Spełnia/Nie spełnia**\* |
| 4. | Funkcjonalności podstawowe i uzupełniające | System powinien realizować co najmniej poniższe funkcjonalności:  Tryb auto-uczenia - przyspieszający i ułatwiający implementację Podział obciążenia na kilkanaście serwerów (loadballancing) Akcelerację SSL dla wybranych serwisów w centrum danych Możliwość analizy poszczególnych rodzajów ruchu w oparciu o profile bezpieczeństwa (profil to obiekt określający zbiór ustawień zabezpieczających aplikacje)  Firewall XML realizujący z możliwością routingu w oparciu o kontent, walidacją schematów XML oraz weryfikacją WDSL. Firewall aplikacji webowych chroniący przed takimi zagrożeniami jak:  • SQL and OS Command Injection  • Cross Site Scripting (XSS)  • Cross Site Request Forgery  • Outbound Data Leakage  • HTTP Request Smuggling  • Buffer Overflow  • Encoding Attacks  • Cookie Tampering / Poisoning  • Session Hijacking  • Broken Access Control j  • Forceful Browsing /Directory Traversal  Oraz innymi podatnościami specyfi kowanym i przez listę OWASP Top 10. | **Spełnia/Nie spełnia**\* |
| 5. | Parametry wydajnościowe | Urządzenie musi prawidłowo obsługiwać przepustowość dla ruchu http - min 100 Mbps | **Spełnia/Nie spełnia**\* |
| 6. | Sygnatury, subskrypcje | Aktualizacja baz sygnatur powinna być systematycznie aktualizowana zgodnie ze zdefiniowanych harmonogramem (Scheduler) | **Spełnia/Nie spełnia**\* |
| 7. | Zarządzanie | Lokalny graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH | **Spełnia/Nie spełnia**\* |
| 8. | Zasilanie | Zasilanie z sieci 230V/50Hz. | **Spełnia/Nie spełnia**\* |
| 9. | Oprogramowanie | oprogramowanie typu antywirus, web security service, IP reputation service, licencje minimum na 12 miesięcy  Możliwosć aktualizacji firmware przez minimum na 12 miesięcy | **Spełnia/Nie spełnia**\* |

1. FortiGate 800C – 2szt.

Wymagane parametry równoważności:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | | **Dane techniczne oferowanego sprzętu**  *(\*niepotrzebne skreślić, a wymagane pola uzupełnić)* |
| **Oferowane urządzenia:**  **Producent: ……………………………………………………………………**  **Model: ………………………………………………………………………..**  **Rok produkcji: ………………………………………………………………**  (**\****należy uzupełnić wszystkie wykropkowane pola)* | | |  |
|  | | | |
| 1. | Architektura systemu ochrony | System ochrony musi być zbudowany przy użyciu minimalnej ilości elementów ruchomych, krytycznych dla jego działania.  Dlatego, główne urządzenie ochronne [gateway] nie może posiadać twardego dysku, w zamian używać pamięci FLASH.  Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizoanego układu ASIC.  Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie). | **Spełnia/Nie spełnia**\* |
|  | System operacyjny | Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia. | *Nazwa systemu operacyjnego:* …………………….………  **Spełnia/Nie spełnia**\* |
|  | Ilość/rodzaj portów | Nie mniej niż 2 porty 10-GbE SFP+, 12 portów Ethernet 10/100/1000 Base-TX, 8 portów współdzielonych 10/100/1000 RJ45 lub SFP, 2 pary portów z funkcją Bypass Protection. | *Ilość portów 10-GbE SFP+:*  *………………….*  *Ilość portów Ethernet 10/100/1000 Base-TX: …….*  *Ilość portów współdzielonych 10/100/1000 RJ45 lub SFP:*  *……*  *Ilość par portów z funkcją Bypass Protection: ………*  **Spełnia/Nie spełnia**\* |
|  | Funkcjonalności podstawowe i uzupełniające | System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych:   1. kontrolę dostępu - zaporę ogniową klasy Stateful Inspection 2. ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM, SMTPS, POP3S, IMAPS, HTTPS) 3. poufność danych - IPSec VPN oraz SSL VPN 4. ochronę przed atakami - Intrusion Prevention System [IPS/IDS]   oraz funkcjonalności uzupełniających:   1. kontrolę treści – Web Filter [WF] 2. kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP, SMTPS, POP3S, IMAPS) 3. kontrolę pasma oraz ruchu [QoS i Traffic shaping] 4. kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM oraz P2P) 5. zapobieganie przed wyciekiem informacji poufnej DLP (Data Leak Preention) 6. SSL proxy z możliwością pełniej analizy szyfrowanej komunikacji dla wybranych protokołów | **Spełnia/Nie spełnia**\* |
|  | Zasada działania (tryby) | Urządzenie powinno dawać możliwość ustawienia jednego z dwóch trybów pracy:  jako router/NAT (3.warstwa ISO-OSI) lub  jako most /transparent bridge/ . Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu. | **Spełnia/Nie spełnia**\* |
|  | Polityka bezpieczeństwa (firewall) | Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, domeny, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasmo gwarantowane i maksymalne, priorytety, oznaczenia DiffServ). | **Spełnia/Nie spełnia**\* |
|  | Wykrywanie ataków | Wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP.   * + Nie mniej niż 3900 sygnatur ataków.   + Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie   + Możliwość wykrywania anomalii protokołów i ruchu | *Ilość sygnatur ataków:………*  **Spełnia/Nie spełnia**\* |
|  | Translacja adresów | Statyczna i dynamiczna translacja adresów (NAT).  Translacja NAPT. | **Spełnia/Nie spełnia\*** |
|  | Wirtualizacja i routing dynamiczny | Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne tabele routingu, polityki bezpieczeństwa i dostęp administracyjny.  Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego.  Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM. | *Ilość możliwych do zdefiniowania w urządzeniu wirtualnych firewalli bez dodatkowych licencji:………*  *Obsługiwane protokoły routingu dynamicznego: ………………………………….*  **Spełnia/Nie spełnia**\* |
|  | Połączenia VPN | Wymagane nie mniej niż:   1. Tworzenie połączeń w topologii Site-to-site oraz Client-to-site 2. Dostawca musi udostępniać klienta VPN własnej produkcji realizującego następujące mechanizmy ochrony końcówki:    1. firewall    2. antywirus    3. web filtering    4. antyspam 3. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności 4. Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN) 5. Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth | **Spełnia/Nie spełnia**\* |
|  | Uwierzytelnianie użytkowników | System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:   1. haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia 2. haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP 3. haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych   Rozwiązanie powinno umożliwiać budowę logowania Single Sign On w środowisku Active Directory bez dodatkowych opłat licencyjnych. | **Spełnia/Nie spełnia**\* |
|  | Wydajność | Obsługa nie mniej niż 7 milionów jednoczesnych połączeń i 190 000 nowych połączeń na sekundę.  Przepływność nie mniejsza niż 20 Gbps dla ruchu nieszyfrowanego i 8 Gbps dla VPN (3DES).  Obsługa nie mniej niż 10 000 jednoczesnych tuneli VPN. | *Ilość jednoczesnych połączeń: …………….*  *Ilość nowych połączeń na sekundę: ……………….*  *Przepływność dla ruchu nieszyfrowanego: ………….*  *Przepływność dla ruchu VPN: ………………….*  *Ilość obsługiwanych jednoczesnych tuneli VPN: ……………………….*  **Spełnia/Nie spełnia**\* |
|  | Funkcjonalność zapewniająca niezawodność | Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive | **Spełnia/Nie spełnia**\* |
|  | Zasilanie | Zasilanie z sieci 230V/50Hz. | **Spełnia/Nie spełnia**\* |
|  | Konfiguracja i zarządzanie | Możliwość konfiguracji poprzez terminal i linię komend oraz konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą:   1. haseł statycznych 2. haseł dynamicznych (RADIUS, RSA SecureID)   System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB. | **Spełnia/Nie spełnia**\* |
|  | Zarządzanie | Ze względu na instniejącą infrastrukturę Zamawiajacego, urządzenie musi być w pełni kompatybilne (tj. istnieje możliwość pełnego konfigurowania jego funkcji i zarządzania nim i monitorowania obciążenia) z urządzeniem FortiManager w wersji oprogramowania min. **v4 MR3 Patch 7** | *Urządzenie jest pełni kompatybilne (tj. istnieje możliwość pełnego konfigurowania jego funkcji i zarządzania nim i monitorowania obciążenia) z urządzeniem FortiManager w wersji oprogramowania: ……………*  **Spełnia/Nie spełnia**\* |
|  | Raportowanie | Ze względu na instniejącą infrastrukturę Zamawiajacego, urządzenie musi być w pełni kompatybilne (tj. istnieje możliwość zbierania logów z urządzeń, generowania raportów, skanowania podatności stacji w sieci, zdalną kwarantannę dla modułu antywirusowego) z urządzeniem FortiAnalyzer w wersji oprogramowania min. **v4 MR3 Patch 7** | *Urządzenie jest w pełni kompatybilne (tj.* *istnieje możliwość zbierania logów z urządzeń, generowania raportów, skanowania podatności stacji w sieci, zdalną kwarantannę dla modułu antywirusowego) z urządzeniem FortiAnalyzer w wersji oprogramowania: ………………….*  **Spełnia/Nie spełnia**\* |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagania dotyczące spełniania przez oferowane urządzenia równoważne odpowiednich norm jakości, warunków gwarancji oraz serwisu** | | **Dokumenty oraz wymogi odnośnie gwarancji i serwisu**  *(\*niepotrzebne skreślić,  a wymagane pola uzupełnić)* |
| 1. | Certyfikaty | Oferowane urządzenia muszą posiadać:  **Certyfikat ISO 9001:2008 lub równoważny dla producenta sprzętu** *(załączyć do oferty dokument potwierdzający spełnianie wymogu wraz z tłumaczeniem na język polski poświadczonym przez Wykonawcę)*  **Deklaracja zgodności CE** *(załączyć do oferty dokument potwierdzający spełnianie wymogu wraz z tłumaczeniem na język polski poświadczonym przez Wykonawcę)*  **Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych** *(załączyć do oferty dokument potwierdzający spełnianie wymogu wraz z tłumaczeniem na język polski poświadczonym przez Wykonawcę)*  **Certyfikat ICSA Labs dla producenta sprzętu dla funkcji: Firewall, IPSec, Network IPS, Antywirus**  *(załączyć do oferty dokument potwierdzający spełnianie wymogu wraz z tłumaczeniem na język polski poświadczonym przez Wykonawcę)*  **Certyfikat UTM NSS Approved dla oferowanych urządzeń**  *(załączyć do oferty dokument potwierdzający spełnianie wymogu wraz z tłumaczeniem na język polski poświadczonym przez Wykonawcę)*  **Certyfikat EAL4+ dla oferowanych urządzeń**  *(załączyć do oferty dokument potwierdzający spełnianie wymogu wraz z tłumaczeniem na język polski poświadczonym przez Wykonawcę)* | *Certyfikat ISO dla producenta:*  **Tak/Nie\***  *Deklaracja zgodności CE:*  **Tak/Nie\***  *Potwierdzenie spełnienia ROHS:*  **Tak/Nie\***  **Spełnia/Nie spełnia\***  *Certyfikat ICSA Labs dla producenta:*  **Tak/Nie\***  *Certyfikat UTM NSS Approved dla urządzeń:*  **Tak/Nie\***  *Certyfikat EAL4+ dla urządzeń:*  **Tak/Nie\*** |
| 2 | Gwarancja, serwis | Urządzenia powinny być objęte serwisem gwarancyjnym producenta przez okres min. 12 miesięcy.  Urządzenia powinny mieć ważne subskrypcje dla wszystkich funkcji ochronnych przez okres min. 12 miesięcy.  Wykonawca zapewni wizytę certyfikowanego inżyniera w siedzibie Zamawiającego celem zweryfikowania poprawności konfiguracji i działania oferowanych rozwiązań, nie rzadziej niż jedna na kwartał w trakcie trwania serwisu gwarancyjnego.  **Firma serwisująca musi posiadać certyfikat ISO 9001:2008 lub równoważny na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń**  *(załączyć do oferty dokument potwierdzający spełnianie wymogu wraz z tłumaczeniem na język polski poświadczonym przez Wykonawcę).*  **Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta- wymagane oświadczenie Wykonawcy potwierdzające, że serwis będzie realizowany przez producenta lub autoryzowanego partnera serwisowego producenta** *(załączyć do oferty oświadczenie)*.  Możliwość przedłużenia gwarancji, serwisu oraz subskrypcji o kolejne lata. | *Okres gwarancji producenta:……miesięcy*  *Okres ważności subskrypcji:……miesięcy*  *Ilośc wizyt certyfikowanego inżyniera: ……. na kwartał*  *Certyfikat ISO na świadczenie usług serwisowych:* **Tak/Nie\***  *Oświadczenie dot. serwisu:* **Tak/Nie\***  **Spełnia/Nie spełnia**\* |
| 3 | Lokalizacja serwisu producenta | **Zamawiający wymaga, aby serwis sprzętu świadczony był przez organizację serwisową producenta, mającą swoją placówkę serwisową na terenie Polski**  *(załączyć do oferty oświadczenie Wykonawcy lub inny dokument potwierdzający spełnienie wymogu).* | **Spełnia/Nie spełnia**\* |

……………………………………….

(data, imię i nazwisko oraz podpis upoważnionego przedstawiciela Wykonawcy)

1. Dotyczy Wykonawcy oferującego rozwiązanie równoważne [↑](#footnote-ref-1)