25 lat
Agencja Restrukturyzacji
i Modernizacji Rolnictwa

adres korespondencyjny
Centrala ARiMR
ul. Poleczki 33, 02-822 Warszawa

Zastępca Prezesa
Sebastian Jaworski

Wykonawcy

Wasze pismo z dnia:	Znak:	Nasz znak:	Data:
		ZP. 126 .DPiZP.2610.27.2019.BS	24 .10.2019 r.

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na „**Zakup urządzeń Firewall wraz z 36 miesięczną gwarancją i konsultacjami**".

Działając na podstawie art. 38 ust. 1 i 1a ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 1843 dalej: „ustawa") Agencja Restrukturyzacji i Modernizacji Rolnictwa z siedzibą w Warszawie przy Al. Jana Pawła II nr 70, zwana w dalszej treści pisma „Zamawiającym", udziela odpowiedzi na pytania zgłoszone w przedmiotowym postępowaniu.

Pytanie nr 1
Pytania dotyczą Załącznika nr 1 do Umowy - Specyfikacja Sprzętu IT i Oprogramowania oraz zasad wdrożenia:

Tabela wymagania minimalne punkt 2:

Czy zamawiający dopuszcza możliwość wykorzystania interfejsów 40Gbit's w chwili zamówienia oraz dostarczenie interfejsów 100Gbit's w kwietniu 2020 (zgodnie z roadmapą)?
Odpowiedź:
Zamawiający informuje, że nie zmienia zapisów SIWZ.

Pytanie nr 2
Pytania dotyczą Załącznika nr 1 do Umowy - Specyfikacja Sprzętu IT i Oprogramowania oraz zasad wdrożenia:

Tabela wymagania minimalne punkt 3

Czy zamawiający zgadza się aby, ze względu na architekturę systemu, logi i raporty przechowywane były z wykorzystaniem dysków 2TB (RAID 1) na komponencie centralnym t.j. Log Server zamiast na urządzeniu końcowym?

Takie podejście pozwala na dużą elastyczność ponieważ serwer taki można wyposażyć w dowolną ilość pamięci dyskowej do przechowywania logów. Ponadto, dostęp do logów zapewniony jest nawet w przypadku fizycznego uszkodzenia urządzenia końcowego.
Odpowiedź:
Zamawiający informuje, że nie zmienia zapisów SIWZ.

Pytanie nr 3
Pytania dotyczą Załącznika nr 1 do Umowy - Specyfikacja Sprzętu IT i Oprogramowania oraz zasad wdrożenia:

Tabela wymagania minimalne punkt 4

Czy zamawiający dopuszcza sposób konfiguracji, gdzie dowolny port sieciowy może być zdefiniowany jako port zarządzania?

Ponadto, czy zamawiający dopuszcza możliwość, aby jedna logiczna instancja systemu (wirtualny kontekst) posiadała jedną tablicę routingu?

Odpowiedź:
Zamawiający wyjaśnia, że dopuszcza powyższe z zastrzeżeniem parametru zawartego w punkcie 16.2 Załącznika nr 1 do wzoru Umowy - Specyfikacja Sprzętu IT i Oprogramowania oraz zasady Wdrożenia stanowiącego Załącznik nr 6 do SIWZ.

Pytanie nr 4
Pytania dotyczą Załącznika nr 1 do Umowy - Specyfikacja Sprzętu IT i Oprogramowania oraz zasad wdrożenia:

Tabela wymagania minimalne punkt 23.

Czy zamawiający dopuszcza sytuację, w której odrębny profil AV, IPS, URL, blokowanie plików, stosowany jest per logiczna instancja systemu (wirtualny kontekst)?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza zmiany parametru w powyższym zakresie i nie zmienia zapisów SIWZ.

Pytanie nr 5
Pytania dotyczą Załącznika nr 1 do Umowy - Specyfikacja Sprzętu IT i Oprogramowania oraz zasad wdrożenia:

Tabela wymagania minimalne punkt 31.

Czy zamawiający potraktuje wymaganie dotyczące łączenia nazw użytkowników z adresami IP, dla systemów Linux lub Unix, jako opcjonalne?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego wymagania jako opcjonalnego i nie zmienia zapisów SIWZ.

Pytanie nr 6
Pytania dotyczą Załącznika nr 1 do Umowy - Specyfikacja Sprzętu IT i Oprogramowania oraz zasad wdrożenia:

Tabela wymagania minimalne punkt 33.

Czy zamawiający potraktuje wymaganie dotyczące skanowania protokołu SMB przez moduł AV jako opcjonalne?

Zgodnie z dobrymi praktykami, zaleca się całkowite blokowanie protokołu SMB na urządzenia firewall zainstalowanym na brzegu sieci

Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego wymagania jako opcjonalnego i nie zmienia zapisów SIWZ.

Pytanie nr 7
Pytania dotyczą Załącznika nr 1 do Umowy - Specyfikacja Sprzętu IT i Oprogramowania oraz zasad wdrożenia:

Tabela wymagania minimalne punkt 35.

Czy zamawiający potraktuje wymaganie dotyczące funkcji Sinkhole jako opcjonalne?

Według naszej najlepszej wiedzy, stosowanie mechanizmu Sinkhole obarczone jest dużą ilością tzw. false-positives.

Wykorzystanie mechanizmu pobierania list adresów IP o potwierdzonej złej reputacji oraz wykorzystanie wspomnianych list w polityce kontroli dostępu.
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego wymagania jako opcjonalnego i nie zmienia zapisów SIWZ.

Pytanie nr 8
Pytania dotyczą Załącznika nr 1 do Umowy - Specyfikacja Sprzętu IT i Oprogramowania oraz zasad wdrożenia:

Tabela wymagania minimalne punkt 37.

Czy zamawiający potraktuje wymaganie dotyczące tworzenia własnych kategorii filtrowania stron WWW jako opcjonalne, jeśli z rozwiązaniem dostarczony zostanie jeden z najbardziej rozbudowanych i skutecznych silników kategoryzacji stron zawierający wbudowaną bazę kategorii?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego wymagania jako opcjonalnego i nie zmienia zapisów SIWZ.

Pytanie nr 9
Pytania dotyczą Załącznika nr 1 do Umowy - Specyfikacja Sprzętu IT i Oprogramowania oraz zasad wdrożenia:

Tabela wymagania minimalne punkt 40.

Czy zamawiający potraktuje wymaganie dotyczące sekwencji uwierzytelniania jako opcjonalne przy zachowaniu bazy lokalnej, LDAP oraz RADIUS jako niezależnych metod uwierzytelniania?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego wymagania jako opcjonalnego i nie zmienia zapisów SIWZ.

Pytanie nr 10
Pytania dotyczą Załącznika nr 1 do Umowy - Specyfikacja Sprzętu IT i Oprogramowania oraz zasad wdrożenia:

Tabela wymagania minimalne punkt 42.

Czy zamawiający zgadza się aby wersje konfiguracji przechowywane były na serwerze zarządzania zamiast na urządzeniu końcowym?

Zaletą jest dostęp do konfiguracji urządzenia nawet w wypadku jego fizycznego uszkodzenia. Ułatwia to również wymianę urządzenia na nowe.
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego wymagania i nie zmienia zapisów SIWZ.

Pytanie nr 11
W Tabeli nr 2 - Wymagania dodatkowo punktowane w ramach kryterium „Parametry techniczne sprzętu IT" Zamawiający wymienił szereg wymaganych funkcji. W p. 7,8,9 Zamawiający wskazał, że wymaganie dotyczy systemu zarządzania, w p.6 wymaganie dotyczy urządzenia firewall. Jednocześnie Zamawiający nie wskazał jednoznacznie, których elementów dotyczą wymagania 1-5. Z ich treści można jednak wnioskować, iż są to dodatkowe wymagania dla urządzeń firewall. Prosimy o jednoznaczne potwierdzenie, iż wymagania 1-5 dotyczą samych urządzeń firewall.
Odpowiedź:
Zamawiający potwierdza, że wymagania dodatkowo punktowane w ramach kryterium „Parametry techniczne Sprzętu IT" zawarte w wierszu „Lp. 1- 5" dotyczą Firewall'i.

Pytanie nr 12
W Tabeli nr 1B - System zarządzania - Zamawiający w punkcie 1.2 stwierdza:
„Dopuszcza się budowę systemy w oparciu o kilka komponentów zarządzania oferowanych przed producenta Firewall- i i systemu zarządzania pod warunkiem iż będą pochodziły od jednego producenta i będą przez niego w całości serwisowane".
Dodatkowo w punkcie 3 stwierdza:

"
System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne
1. *obsługa nie mniej niż 10 firewalli fizycznych*
2. *obsługa nie mniej niż 100 firewalli wirtualnych*
3. *zapewnienie obsługi przestrzeni dyskowej o pojemności nie mniejszej niż 10 TB.*

Możliwość rozbudowy o dodatkową przestrzeń dyskową przeznaczonej na logowanie (dopuszcza się rozbudowę poprzez dokupienie dodatkowej licencji)"
Prosimy o jednoznaczne potwierdzenie, iż powyższe wymaganie opisane w punkcie 3 dotyczy wszystkich komponentów tworzących system zarządzania
Odpowiedź:
Zamawiający potwierdza, że wymaganie opisane w punkcie 3 Tabeli nr 1B – System zarzadzania, dotyczy wszystkich komponentów tworzących system zarządzania, przy czym w zacytowanym punkcie 3.2 zapis brzmi „obsługa nie mniej niż **10** firewalli wirtualnych".

Pytanie nr 13
Dotyczy wymagania nr 2 z Tabeli 1A. Czy Zamawiający dopuści urządzenie, które będzie wyposażone w 16 portów 1/10G SFP+ wyposażonych w 12 wkładek 10GB-SR, 4 porty 40G QSFP+ i będzie posiadało możliwość rozbudowy poprzez wymianę 4 portów 40G na:
a. 8 x 1/10G SFP+
b. 8 x 1G RJ-45
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego wymagania i nie zmienia zapisów SIWZ.

Pytanie nr 14
Dotyczy wymagania nr 3 z Tabeli 1A. Czy Zamawiający dopuści urządzenie z dyskiem 800GB SSD skoro logi mają być wysyłane do centralnego systemu zarządzania?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego wymagania i nie zmienia zapisów SIWZ.

Pytanie nr 15
Dotyczy wymagania nr 7 z Tabeli 1A. Czy mając na uwadze fakt, iż wymaganie to wskazuje jednoznacznie na zapisy z dokumentacji technicznej urządzeń jednego producenta Palo Alto
– Zamawiający dopuści rozwiązania nierealizujące tych wymogów a pochodzące od wiodącego producenta urządzeń typu firewall?
Odpowiedź:
Zamawiający informuje, że nie zmienia zapisów SIWZ.

Pytanie nr 16
Dotyczy wymagania nr 10.2 z Tabeli 1A. Czy Zamawiający dopuści rozwiązanie, które nie posiada funkcjonalności routed-based VPN, ale posiada pozostałe funkcjonalności w zakresie realizacji VPN?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 17
Dotyczy wymagania nr 11.2 z Tabeli 1A. Wg danych ze Sprawozdania z działalności Agencji Restrukturyzacji i Modernizacji Rolnictwa za 2018 rok w organizacji Zamawiającego zatrudnionych jest 11 121 osób. Nie jest możliwe, żeby wszystkie te osoby jednocześnie potrzebowały korzystać z połączenia VPN. Prosimy o urealnienie liczby potrzebnych licencji VPN do liczby jednoczesnych połączeń, które zwykle szacuje się w organizacjach na poziomie kilku procent liczby zatrudnionych.
Odpowiedź:
Zamawiający działając na podstawie art. 38 ust. 4 ustawy wprowadza następującą zmianę w treści siwz tj.:

1) **W Załączniku nr 1 do SIWZ, w Tabeli nr 1A, w wierszu „Lp. 11" wymagania otrzymują brzmienie:**
„1.Firewall musi spełniać następujące parametry wydajnościowe:
a) minimum 15Gbps **przepustowości dla ruchu IPSec**
b) minimum **5 000** tuneli IPSEC VPN (site-to-site)
c) minimum **10 000** tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN.
2.Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji lub jeżeli dedykowany klient VPN (dla systemów: Windows, Linux, Android, MacOS) oferowany przez producenta Sprzętu IT wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla **3 000** jednoczesnych użytkowników."

2) **W Załączniku nr 1 do wzoru Umowy stanowiącej załącznik nr 6 do SIWZ, w tabeli dla „Firewall'e – 2 szt., każde spełniające następujące wymagania minimalne" w wierszu „Lp. 11" wymagania otrzymują brzmienie:**
„1.Firewall musi spełniać następujące parametry wydajnościowe:
a) minimum 15Gbps **przepustowości dla ruchu IPSec**
b) minimum **5 000** tuneli IPSEC VPN (site-to-site)
c) minimum **10 000** tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN.
2.Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji lub jeżeli dedykowany klient VPN (dla systemów: Windows, Linux, Android, MacOS) oferowany przez producenta Sprzętu IT wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla **3 000** jednoczesnych użytkowników."

Pytanie nr 18
Dotyczy wymagania nr 12.1 z Tabeli 1A. Nie znajdujemy powiązania pomiędzy MFA a politykami z punktu 12.1. Prosimy o wyjaśnienie w jaki sposób według Zamawiającego MFA może być zastosowane do polityki z np. kategoriami URL? Prosimy o modyfikację zapisów SIWZ w tym zakresie.
Odpowiedź:
Zamawiający wyjaśnia, że dostęp do określonej kategorii zasobów (informacji) może być zabezpieczony uwierzytelnieniem się przez MFA.

Pytanie nr 19
Dotyczy wymagania nr 17 z Tabeli 1A. Czy Zamawiający dopuści rozwiązanie z maksymalną liczbą 18 wirtualnych kontekstów?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 20
Dotyczy wymagania nr 21.2 z Tabeli 1A. Czy Zamawiający dopuści rozwiązanie, które spełnia wymagania minimalne w zakresie wydajności kontroli firewalla stanowego i kontroli aplikacji, ale nie jest taka sama? Wymaganie w obecnym kształcie dyskryminuje rozwiązania wszystkich innych producentów poza Palo Alto, które mają większą wydajność.
Odpowiedź:
Zamawiający działając na podstawie art. 38 ust. 4 ustawy wprowadza następującą zmianę w treści siwz tj.:

1) **W Załączniku nr 1 do SIWZ, w Tabeli nr 1A, w wierszu „Lp. 21" wymaganie w punkcie 2 otrzymuje brzmienie:**
„2. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewalla stanowego i kontroli aplikacji musi wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych."
2) **W Załączniku nr 1 do wzoru Umowy stanowiącej załącznik nr 6 do SIWZ, w tabeli dla „Firewall'e – 2 szt., każde spełniające następujące wymagania minimalne" w wierszu „Lp. 21" wymaganie w punkcie 2 otrzymuje brzmienie:**
„2. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewalla stanowego i kontroli aplikacji musi wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych."

Pytanie nr 21
Dotyczy wymagania nr 22 z Tabeli 1A. W punkcie 1 Zamawiający oczekuje, żeby informacja o aplikacji była traktowana jako atrybut, a nie „wartość", a w punkcie 2 oczekuje, żeby była traktowana jako „wartość". Mając na uwadze powyższe wnosimy o usunięcie przedmiotowego zapisu z tabeli 1A gdyż poza wykluczeniem merytorycznym ppkt. 1 i 2 wskazują one jednoznacznie na zapisy z dokumentacji technicznej urządzeń jednego producenta Palo Alto.
Odpowiedź:
Zamawiający informuje, że nie zmienia zapisów SIWZ.

Pytanie nr 22
Dotyczy wymagania nr 23.1 z Tabeli 1A. Czy Zamawiający dopuści rozwiązanie, które nie posiada możliwości blokowania plików per aplikacji, gdyż wymaganie to wskazuje jednoznacznie na zapisy z dokumentacji technicznej urządzeń jednego producenta Palo Alto?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 23
Dotyczy wymagania nr 24.1 z Tabeli 1A. Czy Zamawiający dopuści rozwiązanie, które nie posiada funkcjonalności blokowania plików typu tif i hta, gdyż wymaganie to wskazuje jednoznacznie na zapisy z dokumentacji technicznej urządzeń jednego producenta Palo Alto?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 24
Dotyczy wymagania nr 24.2 z Tabeli 1A. Czy Zamawiający dopuści rozwiązanie, które nie posiada możliwości rozpoznawania za pomocą MIME, ale za pomocą tzw. „magic numbers" które jest skuteczniejszą metodą implementowaną przez wszystkich wiodących producentów firewalli.
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 25
Dotyczy wymagania nr 28 z Tabeli 1A. Czy Zamawiający dopuści rozwiązanie, które nie posiada funkcjonalności inspekcji szyfrowanej komunikacji SSH, gdyż wymaganie to wskazuje jednoznacznie na zapisy z dokumentacji technicznej urządzeń jednego producenta Palo Alto?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 26
Dotyczy wymagania nr 31 z Tabeli 1A. Czy Zamawiający dopuści rozwiązanie, które nie posiada funkcjonalności śledzenia użytkowników na podstawie wiadomości z syslog, ale posiada możliwość integracji z system kontroli NAC (np. Cisco ISE) i może wykonywać po integracji z takim systemem znacznie dokładniejsze śledzenie?
Odpowiedź:
Zamawiający wyjaśnia, że w punkcie 3 wymagania 31 jest zapis o treści: „3. Dopuszcza się zastosowanie innego mechanizmu wbudowanego w Firewall który technicznie pozwoli na uzyskanie równoważnej funkcjonalności dotyczącej „śledzenia" logowania użytkowników.", dopuszczające rozwiązanie alternatywne.

Pytanie nr 27
Dotyczy wymagania nr 33 z Tabeli 1A. Czy Zamawiający dopuści rozwiązanie nie posiadające funkcjonalności AV, ale posiadające funkcjonalność Antymalware?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 28
Dotyczy wymagania nr 33.2 i 34.2 z Tabeli 1A. Czy Zamawiający dopuści rozwiązanie, w którym funkcjonalność Antymalware jest realizowana z chmury zamiast z lokalnej bazy sygnatur? Rozpoznawanie w chmurze jest zdecydowanie skuteczniejsze i implementowane w najlepszych rozwiązaniach wiodących producentów urządzeń firewall. Rozpoznawanie lokalne jest zdecydowanie słabszym rozwiązaniem.
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 29
Dotyczy wymagania nr 34.1 z Tabeli 1A. Czy Zamawiający dopuści rozwiązanie nie posiadające funkcjonalności ochrony przed Spyware, ale posiadające funkcjonalność ochrony przed Malware?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 30
Dotyczy wymagania nr 36 z Tabeli 1A. Czy Zamawiający dopuści rozwiązanie, które funkcjonalność wykrywania sieci typu Botnet realizuje na podstawie analizy przeprowadzonej w chmurze producenta rozwiązania? Jest to zdecydowanie skuteczniejsze rozwiązanie implementowane w najlepszych rozwiązaniach wiodących producentów urządzeń firewall.
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 31
Dotyczy wymagania nr 38 z Tabeli 1A. Czy Zamawiający dopuści rozwiązanie, które funkcjonalność z tego punktu realizuje w chmurze producenta rozwiązania? Jest to zdecydowanie skuteczniejsze rozwiązanie w porównaniu do analizy lokalnej.
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 32
Dotyczy wymagania nr 42 z Tabeli 1A. Czy Zamawiający dopuści rozwiązanie, w którym backupy konfiguracji są zapisywane w systemie zarządzania, który będzie przedmiotem oferty?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 33
Dotyczy wymagania nr 3.3 z Tabeli 1B. Czy Zamawiający dopuści rozwiązanie, w którym powierzchnia dyskowa wynosi 2.2TB?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 34
Dotyczy wymagania nr 6.3 z Tabeli 1B. W punkcie 6.3 Zamawiający oczekuje, że System Zarządzania pozwala na tworzenie raportów na podstawie zbudowanych kontenerów lub grup urządzeń. Funkcjonalność ta występuje jedynie w urządzeniach producenta Palo Alto czy Zamawiający chcąc zachować realną konkurencyjność w przedmiotowym postępowaniu dopuści urządzenia nie posiadające tej funkcjonalności?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 35
Dotyczy SIWZ, Rozdział XI, punk 1.2 (Kryterium „Parametry techniczne Sprzętu IT", tabela, wiersz 4.
Czy Zamawiający przyzna dodatkowe punkty dla rozwiązania, które realizuje funkcjonalność z Poziomu systemu zarządzania, który jest częścią niniejszego postępowania?
Odpowiedź:
Zgodnie z odpowiedzią na pytanie nr 11 wymagania dodatkowo punktowane w ramach kryterium „Parametry techniczne Sprzętu IT" w wierszu „Lp. 1- 5" dotyczą Firewall'i. Zamawiający zauważa, że Wykonawca w Tabeli nr 2 zawartej w Formularzu ofertowym zaznacza tylko sformułowanie „TAK" w przypadku spełnienia wszystkich parametrów technicznych opisanych w danej pozycji lub „NIE" w przypadku ich niespełnienia. Zatem w przypadku zaoferowania rozwiązania realizowanego z poziomu systemu zarzadzania Wykonawca powinien zaznaczyć, „NIE" co oznacza nie spełnienie tego wymagania i oferta takiego wykonawcy otrzyma dla tej pozycji 0 pkt.

Pytanie nr 36
Dotyczy SIWZ, Rozdział XI, punk 1.2 (Kryterium „Parametry techniczne Sprzętu IT", tabela, wiersz 5.
W dzisiejszych czasach zagrożenia cybernetyczne rozprzestrzeniają się z niebywałą prędkością, co pokazują chociaż by ostatnie głośne sprawy ataków typu Ransomware. Jak wiadomo, ataki te wyrządziły najmniejsze szkody i straty finansowe tam, gdzie zasoby były zabezpieczone rozwiązaniami, których producenci w najkrótszym możliwym czasie dostarczali aktualizacji poprawek i sygnatur. W świetle tych wydarzeń, staje się jasne iż przeciąganie z wgrywaniem poprawek bezpieczeństwa niesie za sobą konkretne wymierne finansowo koszty, a co gorsza utratę reputacji instytucji. Dla tego też, w odróżnieniu od rozwiązań starszych generacji, nowoczesne systemy bezpieczeństwa posiadają na bieżąco(nawet kilka razy dziennie) aktualizowane bazy sygnatur i poprawek bezpieczeństwa by nadążyć za ciągle rozwijającymi się zagrożeniami. Pozostawienie możliwości przetestowania aktualizacji w odpowiedzialności administratora niesie ogromne ryzyko, gdyż administrator pojedynczej instytucji najczęściej nie posiada wystarczającej wiedzy na temat chronionych przez system NGFW systemów, a jeszcze mniej wiedzy o aktualnych zagrożeniach i istniejących aktualizacjach sygnatur dotyczących tych systemów. Dodatkowo, administrator nie posiada czasu by testować poprawki bezpieczeństwa i sygnatury aktualizowane kilka razy dziennie. Zważając na powyższe, w świecie dzisiejszych zagrożeń cybernetycznych to do wyspecjalizowanych laboratoriów producentów rozwiązań bezpieczeństwa należy dogłębna weryfikacja poprawności działania sygnatur i opublikowanie zweryfikowanej poprawki możliwie najszybciej.

Tak zdefiniowane wymaganie nie przyczynia się do zwiększenia bezpieczeństwa rozwiązania lecz blokuje możliwość zdobycia dodatkowych punktów dla innych producentów niż Palo Alto Networks. Prosimy zatem o usunięcie wymagania gdyż jest ono sprzeczne z ideą działania nowoczesnych systemów NGFW jak również jest sprzeczne z najlepszymi praktykami przyjętymi w branży.

Odpowiedź:

Zamawiający informuje, że nie zmienia zapisów SIWZ.

Jednocześnie Zamawiający wyjaśnia, że w wymaganiu nie chodzi o poprawki bezpieczeństwa tylko o sygnatury określające aplikacje. Funkcjonalność ma na celu zwiększenie bezpieczeństwa poprzez zweryfikowanie czy uruchomienie nowych sygnatur APLIKACJI (nie sygnatur bezpieczeństwa takich jak AV, IPS, etc), nie wpłynie negatywnie na działanie polityk bezpieczeństwa.

Pytanie nr 37

Dotyczy SIWZ, Rozdział XI, punk 1.2 (Kryterium „Parametry techniczne Sprzętu IT", tabela, wiersz 7.

Pragniemy zwrócić uwagę, iż tylko rozwiązanie Palo Alto ma taki sam graficzny interfejs systemu zarządzania Panorama jak urządzenia Firewall. Najczęściej systemy zarządzania posiadają interfejsy przygotowane w ten sposób by usprawnić zarządzanie wieloma urządzeniami firewall. To producent posiada najlepszą wiedzę o swoich urządzeniach o ich możliwościach i funkcjonalnościach, i to producent zatrudniający zespoły inżynierów i projektantów ustala możliwy sposób zarządzania funkcjonalnościami wielu urządzeń przy czym producent zawsze dąży do największego usprawnienia systemu i ułatwienia dla administratorów.

Prosimy zatem o usunięcie wymagania gdyż tak zdefiniowane wymaganie nie przyczynia się do zwiększenia bezpieczeństwa rozwiązania lecz napisane by blokować możliwość zdobycia dodatkowych punktów dla innych producentów niż Palo Alto Networks.

Odpowiedź:

Zamawiający informuje, że nie zmienia zapisów SIWZ.

Pytanie nr 38

Dotyczy SIWZ, Rozdział XI, punk 1.2 (Kryterium „Parametry techniczne Sprzętu IT", tabela, wiersz 8.

Punkt może być spełniony tylko przez rozwiązanie Panorama producenta PaloAlto Network.

Prosimy o usunięcie wymagania gdyż tak zdefiniowane wymaganie nie przyczynia się do zwiększenia bezpieczeństwa rozwiązania lecz napisane by blokować możliwość zdobycia dodatkowych punktów dla innych producentów niż Palo Alto Networks.

Odpowiedź:

Zamawiający informuje, że nie zmienia zapisów SIWZ.

Pytanie nr 39

Dotyczy Załącznik 1 formularz ofertowy, tabeli nr 1A, wymaganie 3.

W punkcie 3 Tableli 1A OPZ Zamawiający pisze: Firewall musi być wyposażony w twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 2TB jednocześnie w punkcie 3.3 tabeli 1B OPZ Zamawiający wymaga dostarczenia systemu zarzadzania i logowania, który zapewnia obsługę przestrzeni dyskowej o pojemności nie mniej iż 10TB.

Z uwagi na fakt, że Zamawiający wymaga 2 urządzenia firewall, wskazane jest aby urządzenia te były wyposażone w centralny system gromadzenia i przetwarzania logów oraz generowania raportów.

Prosimy o dopuszczenie rozwiązania, które nie posiada lokalnych dysków do przechowywania logów, lecz do długo terminowego przechowywania logów będzie dostarczony centralny system przetwarzania logów spełniający wymagania opisane w Tabeli 1B.

Odpowiedź:

Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 40

Dotyczy Załącznik 1 formularz ofertowy, tabeli nr 1A, wymaganie 10.3.

Proszę potwierdzenie iż „użytkownicy mobilni" to użytkownicy i pracownicy korzystający z urządzeń mobilnych (laptopów, tabletów, itp.)

Odpowiedź:

Zamawiający potwierdza, że przez zapis „użytkownicy mobilni" należy rozumieć użytkowników i pracowników korzystający z urządzeń mobilnych w szczególności takich jak laptopów, tabletów i smartphone'ów.

Pytanie nr 41

Dotyczy Załącznik 1 formularz ofertowy, tabeli nr 1A, wymaganie 11.1.a

Proszę o potwierdzenie iż Zamawiający ma myśli przepustowość połączenia IPSec minimim 15Gbps.

Odpowiedź:

Zgodnie z odpowiedzią na pytanie nr 17.

Pytanie nr 42

Dotyczy Załącznik 1 formularz ofertowy, tabeli nr 1A, wymaganie 17

Czy Zamawiający zaakceptuje rozwiązanie które na etapie dostarczenia posiada możliwość uruchomienia 10 wirtualnych instancji z możliwością rozbudowy nawet do 500 wirtualnych instancji.

Odpowiedź:

Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 43

Dotyczy Załącznik 1 formularz ofertowy, tabela nr 1A, wymaganie 18

Tak skonstruowane pytanie ogranicza możliwość zaoferowania Państwu innych rozwiązań niż rozwiązanie Palo Alto Networks, gdyż możliwość przekierowania ruchu dla wybranych aplikacji i konkretnych użytkowników z pominięciem tablicy routingu jest wspierane wyłącznie przez urządzenia firmy Palo Alto Networks.

Prosimy o dopuszczenie rozwiązania alternatywnego bazującego na możliwości przekierowania ruchu (PBR - policy base routing) z pominięciem tablicy routingu na podstawie poniższych parametrów:

- *Protokół*
- *Źródłowa adresacja IP z maską*
- *Źródłowe porty*
- *Źródłowy Interfejs*
- *Docelowa adresacja IP z maską*
- *Docelowe porty*
- *Docelowy Interfejs*

Odpowiedź:

Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 44

Dotyczy Załącznik 1 formularz ofertowy, tabela nr 1A, wymaganie 31

Powyższe wymaganie w takiej postaci ponownie faworyzuje producenta Palo Alto Networks.

Prosimy o dopuszczenie protokołu RADIUS jako alternatywnego do syslog lub dopuszczenie rozwiązania w którym funkcjonalność będzie realizowana przez zewnętrzny system tego samego producenta w postaci maszyny wirtualnej i natywnie współpracującym z systemem zabezpieczeń firewall, która dokona konwersji syslog – SSO.

Dodatkowo prosimy o informacje: jaka powinna być liczba równoległych sesji SSO dla tego zastosowania? Czy ta maszyna wirtualna może być uruchomiona na zasobach wirtualizacyjnych Zamawiającego ?

Odpowiedź:

Zgodnie z odpowiedzią na pytanie nr 26.

Pytanie nr 45

Dotyczy Załącznik 1 formularz ofertowy, tabela nr 1B, wymaganie 3.1

Proszę o sprecyzowanie czy Zamawiający ma na myśli „10 firewalli fizycznych lub 10 firewalli wirtualnych" co razem daje 10 firewalli dowolnego typu czy Zamawiający ma na myśli „10 firewalli fizycznych i 10 firewalli wirtualnych" co razem daje 20 firewalli dowolnego typu?

Odpowiedź:

Zamawiający wyjaśnia, że każdy punkt jest traktowany jako oddzielny wymóg, a nie alternatywa.

Pytanie nr 46

Dotyczy Załącznik 1 formularz ofertowy, tabela nr 1A, wymaganie 23

Podane zapisy szczegółowo wskazują na producenta Palo Alto Networks. Czy jako równoważny dopuszcza się się system, gdzie traktowanie aplikacji i filtra URL jako parametru polityki, dla których dowiązuje się profile ochronne AV, DNS, IPS?

Odpowiedź:

Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 47

2	Firewall musi być wyposażony w: 1. 4 interfejsy 100/1000/10GE Ethernet (RJ45) 2. 16 interfejsów 1/10GE SFP+ (z czego 12 interfejsów obsadzonych modułami 10GE SFP+ SR) 3. 4 interfejsy 40GE/100GE QSFP+ lub alternatywnie 4 interfejsy 40GE QSFP+ i 4 interfejsy 100GE QSFP+

Czy zamawiający dopuści zastosowanie rozwizania umożliwuającego przesłanie oczekiwanej przez zamawiającego ilości danych z wykorzystaniem standardu IEEE802.3ad?

Odpowiedź:

Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 48

3	Firewall musi być wyposażony w twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 2 TB (RAID 1).

Czy zamawiający zgadza się aby, ze względu na architekturę systemu, logi i raporty przechowywane były z wykorzystaniem dysków 2TB (RAID 1) na komponencie centralnym t.j. Log Server zamiast na urządzeniu końcowym? Takie podejście pozwala na dużą elastyczność ponieważ serwer taki można wyposażyć w dowolną ilość pamięci dyskowej do przechowywania logów. Ponadto, dostęp do logów zapewniony jest nawet w przypadku fizycznego uszkodzenia urządzenia końcowego

Odpowiedź:

Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 49

4	Firewall musi być wyposażony w dedykowany port konsoli/zarządzania. Port ten musi być wydzielony logicznie i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji.

1) Czy zamawiający dopuszcza sposób konfiguracji, gdzie dowolny port sieciowy może być zdefiniowany jako port zarządzania? Ponadto, czy zamawiający dopuszcza możliwość, aby jedna logiczna instancja systemu (wirtualny kontekst) posiadała jedną tablicę routingu? 2)Czy zamawiający dopuści urządzenie którego port do zarządzania nie pracuje w żadnej instancji routingu (tak jak port konsoli RS-232)

Odpowiedź:

1) Zgodnie z odpowiedzią na pytanie nr 3.
2) Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 50

12	Firewall musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach: 1. Polityki definiujące powinny umożliwiać wykorzystanie: a) adresów źródłowych b) adresów docelowych c) użytkowników d) numerów portów usług e) kategorie URL 2. System musi obsługiwać następujące mechanizmy uwierzytelnienia a) RADIUS lub TACACS+ b) LDAP c) Kerberos lub SAML 2.0

Czy zamawiający dopuszcza rozwiązanie, w którym polityki realizowane są w wyniku przekazania do urządzenia firewall informacji użytkowniku (będących wynikiem jego autentykacji) przez agenta zainstalowanego na stacji roboczej użytkownika? Oprogramowanie oraz rozwiązanie firewall są produktami tego samego producenta

Odpowiedź:

Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 51

16	1. Firewall musi obsługiwać nie mniej niż 50 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń.

Według naszej wiedzy powyższy zapis jest ograniczeniem konkurencji, gdyż wspomnianą funkcjonalność posiada tylko jeden producent na rynku jakim jest Palo Alto. Wnosimy o usunięcie zapisu.

Odpowiedź:

Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 52

23	1. Firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. 2. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.

Według naszej wiedzy powyższy zapis jest ograniczeniem konkurencji, gdyż wspomnianą funkcjonalność posiada tylko jeden producent na rynku jakim jest Palo Alto. Wnosimy o usunięcie zapisu.

Odpowiedź:

Zgodnie z odpowiedzią na pytanie nr 22.

Pytanie nr 53

25	1. Firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. 2. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.

Według naszej wiedzy powyższy zapis jest ograniczeniem konkurencji, gdyż wspomnianą funkcjonalność posiada tylko jeden producent na rynku jakim jest Palo Alto. Wnosimy o usunięcie zapisu.
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 54

31	1. Firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia.

Według naszej wiedzy powyższy zapis jest ograniczeniem konkurencji, gdyż wspomnianą funkcjonalność posiada tylko jeden producent na rynku jakim jest Palo Alto. Wnosimy o usunięcie zapisu.
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 55

33	2. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder, w szczególności: http, smtp, imap, pop3, ftp, smb.

Według naszej wiedzy powyższy zapis jest ograniczeniem konkurencji, gdyż wspomnianą funkcjonalność posiada tylko jeden producent na rynku jakim jest Palo Alto. Wnosimy o usunięcie zapisu.
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 56

35	1. Firewall musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). 2. Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).

Czy zamawiający dopuści rozwiązanie realizujące blokowanie dos+ępu do domen o złej reputacji w oparciu o inny mechanizm niż Sinkhole?
Odpowiedź:
Zgodnie z odpowiedzią na pytanie nr 7.

Pytanie nr 57

37	5. Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.

Czy zamawiający dopuści rozwiązanie realizujące dostęp do listy stron, tworzonej przez zamawiającego, bez wykorzystania modułu związanego z kategoryzacją stron?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 58

40	3. Firewall musi zapewniać tworzenie sekwencji uwierzytelniającej posiadającej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).

Czy zamawiający potraktuje wymaganie dotyczące sekwencji uwierzytelniania jako opcjonalne przy zachowaniu bazy lokalnej, LDAP oraz RADIUS jako niezależnych metod uwierzytelniania?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Pytanie nr 59

42	Firewall musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym Firewall-a

Czy zamawiający dopuści rozwiązanie, w którym wszystkie elementy polityk oraz dowolna ilość wcześniejszych wersji polityk dostępna będzie w systemie centralnego zarządzania rozwiązaniami firewall?
Odpowiedź:
Zamawiający informuje, że nie dopuszcza powyższego rozwiązania i nie zmienia zapisów SIWZ.

Zamawiający działając na podstawie art. 38 ust. 4 ustawy wprowadza następujące zmiany:

ZMIANA nr 1 zmiany porządkowe w treści SIWZ (zmiany zaznaczone boldem):

W Załączniku nr 1 do wzoru Umowy stanowiącej załącznik nr 6 do SIWZ, w Tabeli dla Firewall'e:

1. *w wierszu 17 poprawia się **numerację** w następujący sposób:*
   1.1 obecny zapis:
   „2. Polityk bezpieczeństwa obejmujących:
   d) System IPS;
   e) System ochrony antymalware/antyspyware;
   f) System ochrony antywirus;"
   otrzymuje brzmienie:
   „2. Polityk bezpieczeństwa obejmujących:
   a) System IPS;
   b) System ochrony antymalware/antyspyware;
   c) System ochrony antywirus;"
   1.2 *obecny zapis:* „1. Koncentratorów VPN dla zdalnego dostępu."
   otrzymuje brzmienie: **„3.** Koncentratorów VPN dla zdalnego dostępu."

2. *w wierszu 40, w pkt 2 poprawia się **numerację** w następujący sposób:*
   obecny zapis:
   „2. Firewall musi umożliwiać uwierzytelnianie administratorów za pomocą:
   d) bazy lokalnej;
   e) serwera LDAP;
   f) RADIUS lub TACACS+."
   otrzymuje brzmienie:"
   „2. Firewall musi umożliwiać uwierzytelnianie administratorów za pomocą:
   a) bazy lokalnej;
   b) serwera LDAP;
   c) RADIUS lub TACACS+."

ZMIANA nr 2 (zmiany zaznaczone boldem):
W Rozdziale IX.1. Miejsce oraz termin składania ofert i otwarcia ofert, pkt 2 i pkt 3 otrzymują brzmienie:

2. Termin składania ofert upływa w dniu **06.11.2019 r. o godzinie 13:00** Oferty otrzymane przez Zamawiającego po tym terminie zostaną zwrócone po upływie terminu przewidzianego na wniesienie odwołania, po uprzednim zawiadomieniu Wykonawcy o fakcie złożenia oferty po terminie.
3. Otwarcie ofert odbędzie się w dniu **06.11.2019 r. o godzinie 13:15** w biurze Zamawiającego, pod adresem ul. Poleczki 33, 02-822 Warszawa.

W związku z powyższym zmianie ulega Formularz Ofertowy stanowiący załącznik nr 1 do SIWZ. Zmieniony Formularz Ofertowy zamieszczony zostaje w odrębnym pliku word o nazwie „Wzór Formularza Ofertowego po zmianach".

Zamawiający informuje, że udzielone odpowiedzi i wprowadzone zmiany oraz zmieniony załącznik nr 1 do SIWZ są wiążące dla Wykonawców

ZASTĘPCA PREZESA
Sebastian Jaworski

Załącznik nr 1 do SIWZ wzór Formularza Ofertowego

Formularz Ofertowy
DPiZP.2610.27.2019

Ja(my) niżej podpisany(-i) .....

Działając w imieniu i na rzecz .....

.....

W odpowiedzi na ogłoszone postępowanie prowadzone w trybie przetargu nieograniczonego na **„Zakup urządzeń Firewall wraz z 36 miesięczną gwarancją i konsultacjami"**, zgodnie z wymaganiami określonymi w specyfikacji istotnych warunków zamówienia i wzorze Umowy wraz z załącznikami, oferuję(-emy) realizację przedmiotu zamówienia za cenę:

Tabela nr 1A

Firewall'e – 2 szt.

Lp.	Parametry wymagane – minimalne wymagane przez Zamawiającego parametry dla pojedynczego Firewall'a	Parametry oferowane (zaznacza Wykonawca)
1	1. Firewall musi być dostarczony jako dedykowane urządzenie typu appliance, przystosowane do montażu w szafie Rack 19". 2. Całość Sprzętu IT musi być zarządzana przez jednego producenta.	TAK/NIE*
2	Firewall musi być wyposażony w: 1. 4 interfejsy 100/1000/10GE Ethernet (RJ45) 2. 16 interfejsów 1/10GE SFP+ (z czego 12 interfejsów obsadzonych modułami 10GE SFP+ SR) 3. 4 interfejsy 40GE/100GE QSFP+ lub alternatywnie 4 interfejsy 40GE QSFP+ i 4 interfejsy 100GE QSFP+	TAK/NIE*
3	Firewall musi być wyposażony w twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 2 TB (RAID 1).	TAK/NIE*
4	Firewall musi być wyposażony w dedykowany port konsoli/zarządzania. Port ten musi być wydzielony logicznie i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji.	TAK/NIE*
5	Firewall musi spełniać następujące parametry wydajnościowe, jeżeli Firewall może pracować w różnych trybach to jego wydajność musi być mierzona w trybie pracy, który pozwala na uruchomienie wszystkich wymaganych funkcji Sprzętu IT: 1. minimum 40 Gbps dla Firewall/kontroli aplikacji; 2. minimum 20 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji; 3. minimum 280 tys. nowych połączeń na sekundę; 4. minimum 8 000 000 równoległych sesji.	TAK/NIE*
6	Firewall musi umożliwiać działanie w trzech trybach pracy: 1. rutera (tzn. w warstwie 3 modelu OSI); 2. przełącznika (tzn. w warstwie 2 modelu OSI); 3. w trybie pasywnego nasłuchu (sniffer).	TAK/NIE*
7	Tryb pracy Firewall-a musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.).	TAK/NIE*
8	1. Firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN. 2. Firewall musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. 3. Firewall musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3.	TAK/NIE*

9	1. Firewall musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. 2. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.	TAK/NIE*
10	1. Firewall musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. 2. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). 3. Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN	TAK/NIE*
11	1. Firewall musi spełniać następujące parametry wydajnościowe: a) minimum 15Gbps **przepustowości dla ruchu IPSec** b) minimum **5 000** tuneli IPSEC VPN (site-to-site) c) minimum **10 000** tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN. 2. Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji lub jeżeli dedykowany klient VPN (dla systemów: Windows, Linux, Android, MacOS) oferowany przez producenta Sprzętu IT wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla **3 000** jednoczesnych użytkowników.	TAK/NIE*
12	Firewall musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach: 1. Polityki definiujące powinny umożliwiać wykorzystanie: a) adresów źródłowych b) adresów docelowych c) użytkowników d) numerów portów usług e) kategorie URL 2. System musi obsługiwać następujące mechanizmy uwierzytelnienia a) RADIUS lub TACACS+ b) LDAP c) Kerberos lub SAML 2.0	TAK/NIE*
13	Firewall musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie: 1. oznaczania pakietów znacznikami DiffServ; 2. ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego; 3. utworzenia 8 klas ruchu sieciowego; 4. kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników; 5. kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP; 6. przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.	TAK/NIE*
14	Firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP	TAK/NIE*
15	Firewall musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.	TAK/NIE*
16	1. Firewall musi obsługiwać nie mniej niż 50 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. 2. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia oraz odpowiednio większą instalację systemu zarządzania (dotyczy liczby zarządzanych firewalli logicznych).	TAK/NIE*
17	Firewall musi obsługiwać nie mniej niż 25 wirtualnych firewalli/systemów/domen/kontekstów i posiadać możliwość rozbudowy do 75 takich systemów. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych: 1. tablic routingu (przy czym system musi umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń, lub zapewnić odpowiednio więcej systemów wirtualnych); 2. Polityk bezpieczeństwa obejmujących: a) System IPS; b) System ochrony antymalware/antyspyware; c) System ochrony antywirus; 3. Koncentratorów VPN dla zdalnego dostępu.	TAK/NIE*

18	Firewall musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu.	TAK/NIE*
19	1. Firewall musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie firewall-i. 2. Firewall-e w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active.	TAK/NIE*
20	1. Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. 2. Firewall musi umożliwiać zdefiniowanie nie mniej niż 50 000 reguł polityki bezpieczeństwa.	TAK/NIE*
21	1. Identyfikacja aplikacji musi odbywać się poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji Sprzętu IT numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. 2. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewalla stanowego i kontroli aplikacji musi wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych. 3. Firewall musi wykrywać 2500 predefiniowanych aplikacji wspieranych przez producenta (w szczególności: Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na Sprzęcie IT bez użycia zewnętrznych narzędzi.	TAK/NIE*
22	1. Firewall musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. 2. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM) w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce.	TAK/NIE*
23	1. Firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. 2. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.	TAK/NIE*
24	1. Firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. 2. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.	TAK/NIE*
25	1. Firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. 2. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.	TAK/NIE*
26	Firewall musi zapewniać ochronę przed atakami typu „Drive-by-download".	TAK/NIE*
27	1. Firewall musi posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. 2. Wymagana jest obsługa deszyfracji i inspekcji protokołu HTTP/2 zarówno dla ruchu inbound jak i outbound.	TAK/NIE*
28	Firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH	TAK/NIE*
29	Firewall musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: 1. Microsoft Active Directory; 2. usługi katalogowe LDAP; 3. serwery Terminal Services.	TAK/NIE*
30	Polityka kontroli dostępu Firewall-a musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.	TAK/NIE*
31	1. Firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. 2. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. 3. Dopuszcza się zastosowanie innego mechanizmu wbudowanego w Firewall który technicznie pozwoli na uzyskanie równoważnej funkcjonalności dotyczącej „śledzenia" logowania użytkowników.	TAK/NIE*
32	1. Firewall musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. 2. System IPS musi działać w warstwie 7 modelu OSI. 3. Baza sygnatur IPS/IDS musi być przechowywana na Firewall-u, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent Sprzętu IT. 4. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja	TAK/NIE*

	IPS/IDS uruchamiana była per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). 5. Firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na Firewall-u bez użycia zewnętrznych narzędzi.	
33	1. Firewall musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. 2. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder, w szczególności: http, smtp, imap, pop3, ftp, smb. 3. Baza sygnatur AV musi być przechowywana na Firewall-u, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń 4. Moduł AV musi być uruchamiany per reguła polityki bezpieczeństwa firewall. 5. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).	TAK/NIE*
34	1. Firewall musi zapewniać ochronę przed atakami typu Spyware – dopuszcza się by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. 2. Baza sygnatur anty-spyware musi być przechowywana na Firewall-u, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. 3. Reguły/silnik anty-spyware musi być uruchamiany per reguła polityki bezpieczeństwa firewall. 4. Nie jest dopuszczalne, aby funkcja ta była uruchamiana per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). 5. Firewall musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na Firewall-u bez użycia zewnętrznych narzędzi i wsparcia producenta. 6. Dopuszcza się aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnego systemu zarządzania i monitorowania.	TAK/NIE*
35	1. Firewall musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). 2. Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).	TAK/NIE*
36	Firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.	TAK/NIE*
37	1. Firewall musi posiadać funkcjonalność URL Flitering wraz z aktualizacją w okresie gwarancji. 2. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL. 3. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. 4. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per cały Firewall lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). 5. Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. 6. Dopuszcza się aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnego systemu zarządzania i monitorowania.	TAK/NIE*
38	1. Firewall musi posiadać funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem. 2. Firewall musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day. 3. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. Jeżeli funkcja ta wymaga zakupu dodatkowej licencji to nie wymagane jest jej dostarczenie w chwili zakupu Firewalla/i.	TAK/NIE*
39	1. Zarządzanie Firewall-em musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę www. 2. Dostęp do Firewall-a i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).	TAK/NIE*

40	1. System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. 2. Firewall musi umożliwiać uwierzytelnianie administratorów za pomocą: a) bazy lokalnej; b) serwera LDAP; c) RADIUS lub TACACS+. 3. Firewall musi zapewniać tworzenie sekwencji uwierzytelniającej posiadającej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).	TAK/NIE*
41	Firewall musi zapewniać interfejs API (JSON, REST, XML lub inny) będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu Firewall-a bez użycia systemu zarządzania lub linii poleceń (CLI).	TAK/NIE*
42	Firewall musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym Firewall-a.	TAK/NIE*
43	Firewall musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall/kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. w innych systemach wirtualnych.	TAK/NIE*
44	Firewall musi umożliwiać bieżące wysyłanie logów do zewnętrznych serwerów SYSLOG oraz posiadać możliwość wysyłania logów z wykorzystaniem protokołu TCP i zdefiniowana portu docelowego.	TAK/NIE*
45	Firewall musi być wyposażony w zasilacze typu AC pracujące redundantnie.	TAK/NIE*

Uwaga 1

***-niewłaściwe przekreślić.**

Tabela nr 1B

System zarządzania:

Lp.	Parametry wymagane – minimalne wymagane przez Zamawiającego parametry dla systemu zarządzania	Parametry oferowane (zaznacza Wykonawca)
1	1. Wraz z urządzeniami Firewall konieczne jest dostarczenie centralnego systemu zarządzania. 2. Dopuszcza się budowę systemu w oparciu o kilka komponentów zarządzania oferowanych przez producenta Firewall-i i systemu zarządzania pod warunkiem, iż będą one pochodziły od jednego producenta i będą przez niego w całości serwisowane. 3. System zarządzania musi pracować w trybie kolektora logów zbierającego jedynie dane z systemów bezpieczeństwa lub w trybie pełnej analizy w celu optymalizacji procesu zbierania logów.	TAK/NIE**
2	System zarządzania, logowania i raportowania musi zostać dostarczony w postaci maszyny wirtualnej instalowanej w środowisku VMWare.	TAK/NIE**
3	System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne: 1. obsługa nie mniej niż 10 firewalli fizycznych 2. obsługa nie mniej niż 10 firewalli wirtualnych 3. zapewnienie obsługi przestrzeni dyskowej o pojemności nie mniejszej niż 10 TB. 4. Możliwość rozbudowy o dodatkową przestrzeń dyskową przeznaczonej na logowanie (dopuszcza się rozbudowę poprzez dokupienie dodatkowej licencji)	TAK/NIE**
4	1. System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach www. 2. System musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli	TAK/NIE**

5	System zarządzania, logowania i raportowania musi zapewniać narzędzia dla szybkiej i skutecznej analizy informacji w tym: 1. umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych. 2. tworzenie statycznych raportów dopasowanych do wymagań Kupującego. 3. zapisywanie stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób. 4. tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Kupującego z funkcjonalnością „drill-down".	TAK/NIE**
6	System zarządzania, logowania i raportowania musi umożliwiać centralne zarządzanie wieloma firewallami fizycznymi i logicznymi w tym: 1. budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu. a) lokalnych (dla wybranych firewalli lub logicznych systemów firewalla). b) globalnych (dla grup firewalli lub kilku systemów logicznych wybranych firewalli). 2. umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery lub logiczne grupy urządzeń umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów) 3. pozwalać na tworzenie raportów na podstawie zbudowanych kontenerów lub grup urządzeń. 4. umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium. 5. umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych. 6. umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi.	TAK/NIE**
7	System zarządzania, logowania i raportowania musi umożliwiać centralne narzędzia inwentury i audytu oraz zarządzania konfiguracjami w tym musi: 1. umożliwiać dystrybucję i zdalną instalację nowych wersji systemu; 2. umożliwiać tworzenie kopii zapasowych zarządzanych firewalli; 3. umożliwiać dystrybucję i zdalną instalację nowych sygnatur; 4. umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem; 5. pozwalać na zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów; 6. umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone; 7. informować o zmianach konfiguracji systemu.	TAK/NIE**
8	System zarządzania, logowania i raportowania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów.	TAK/NIE**

Uwaga 2

**-niewłaściwe przekreślić

TABELA nr 2 – Wymagania dodatkowe punktowane w ramach kryterium „Parametry techniczne Sprzętu IT"

Lp.	„Parametry techniczne Sprzętu IT" (P_T)	Parametr oferowany zaznacza Wykonawca
1.	Automatycznie identyfikuje aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się poprzez analizę heurystyczną	TAK/NIE***
2.	Blokuje transmisję plików szyfrowanych co najmniej: 1. Dokumentów office (doc, xls, ppt, docx, xlsx, pptx) 2. Plików skompresowanych (zip, rar)	TAK/NIE ***

3.	Wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie sprzętowym/fizycznym	TAK/NIE ***
4.	Posiada koncept konfiguracji kandydackiej którą można dowolnie edytować na Firewall-u bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji Firewall-a do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu w tym: a. Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami. b. Możliwość blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji	TAK/NIE ***
5.	Sprawdzenie wpływu nowo pobranych aktualizacji sygnatur aplikacyjnych (przed ich zatwierdzeniem do użycia) na istniejące polityki bezpieczeństwa – funkcja ta musi być wbudowana w Firewall-a i nie może wymagać korzystania z rozwiązań trzecich	TAK/NIE ***
6.	W przypadku utraty komunikacji z centralnym systemem zarządzania Firewall musi pozwalać na: 1. Lokalne konfigurowanie reguł bezpieczeństwa 2. Lokalne zbieranie i analizowanie logów 3. korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: a. ruchu sieciowym b. aplikacjach c. zagrożeniach d. filtrowaniu stron www 4. tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML 5. tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu	TAK/NIE ***
7.	System zarządzania, logowania i raportowania posiada taki sam graficzny Interfejs Użytkownika (GUI) jak zarządzane Firewall-e	TAK/NIE ***
8.	System zarządzania, logowania i raportowania Firewall-ami umożliwia dystrybucję i zdalną instalację nowych wersji systemu oraz poprawek	TAK/NIE ***
9.	System zarządzania, logowania i raportowania Firewall-i umożliwia zarządzanie posiadanymi przez Zamawiającego urządzeniami Palo Alto Networks PA-5060 w całościowym zakresie opisanym w wymaganiach dla tego systemu	TAK/NIE ***

Uwaga 3:

***- **niewłaściwe przekreślić.** *W przypadku nie przekreślenia żadnego ze zwrotów lub łącznego przekreślenia obu zwrotów „TAK/NIE" przez Wykonawcę dla danej pozycji. Zamawiający uzna że zaoferowany Sprzęt IT nie spełnia parametrów technicznych opisanych i wymaganych w danym kryterium technicznym i oferta takiego Wykonawcy otrzyma dla tej pozycji 0 pkt.*

TABELA nr 3

Oferujemy Sprzęt IT o parametrach technicznych wymienionych w Tabeli nr 1A i nr 1B oraz w Tabeli nr 2 (punktowane w ramach kryteriów oceny ofert****), oraz na warunkach określonych we wzorze Umowy, który stanowi Załącznik nr 6 do SIWZ **za cenę:**
Uwagi:
**** - o ile są oferowane*

Lp.	Przedmiot	Cena ofertowa netto zł	Podatek VAT		Cena ofertowa brutto zł
			%	zł	
	a	b	c	d = b x c	e = b + d
1.	Sprzęt IT (Firewall - 2 szt. wraz z systemem zarządzania) oraz z Oprogramowaniem, spełniający wymagania określone w Tabeli nr 1A, nr 1B i Tabeli nr 2 oraz Serwisem gwarancyjnym świadczonym przez 36 miesięcy wg wymagań zdefiniowanych w § 6 wzoru umowy. ***Producent*** ..... ***Model Firewall***				
2.	Wdrożenie i Dokumentacja powykonawcza, zgodnie z § 7 ust. 1 pkt. 2) wzoru Umowy				
Razem [∑1÷2]:			X		

Tabela nr 4

Lp.	Przedmiot zamówienia	Ilość jednostek	Cena jednostkowa netto (zł) *(cena za 1 godz. konsultacji)*	Cena ofertowa netto (zł)	Podatek VAT		Cena ofertowa brutto (zł)
					%	zł	
[a]	*[b]*	*[c]*	*[d]*	*[e] = [c] x [d]*	*[f]*	*[g] = [e] x [f]*	*[h] = [e] + [g]*
1	Konsultacje, o których mowa w § 2 ust. 4 i 5 wzoru Umowy	500 godz.					

Tabela nr 5 - Łączna cena oferty

Przedmiot		Cena netto [zł]	Podatek VAT [zł]	Cena brutto [zł]
[a]	*[b]*	*[c]*	*[d]*	*[e]*
1	Sprzęt IT (Firewall - 2 szt. wraz z systemem zarządzania) oraz z Oprogramowaniem, spełniający wymagania określone w Tabeli nr 1A, nr 1B i Tabeli nr 2 oraz Serwisem gwarancyjnym świadczonym przez 36 miesięcy wg wymagań zdefiniowanych w § 6 wzoru Umowy oraz Wdrożenie i Dokumentacja powykonawcza, zgodnie z § 7 ust. 1 pkt. 2) wzoru umowy, - **wg Tabeli nr 3** *(należy wpisać odpowiednio wartości z Tabeli nr 3 z pozycji „Razem": kol. „b", „d" i „e")*			
2	Konsultacje, o których mowa w § 2 ust. 4 i 5 wzoru Umowy **– wg Tabeli nr 4** *(należy wpisać odpowiednio wartości z Tabeli nr 4: kol. „e", „g" i „h")*			
Łączna cena oferty [∑1÷2]:				

Łączna cena netto oferty ..... zł słownie: _____

Łączna cena brutto oferty ..... zł słownie: _____

Oświadczamy, że:

1. **Termin dostarczenia Sprzętu IT wraz z Oprogramowaniem, Dokumentów, oraz Wdrożenie, o którym mowa w § 4 ust. 1 wzoru Umowy wyniesie..... Dni Roboczych.**
2. Realizację przedmiotu zamówienia wykonamy w terminach określonych w Rozdziale II SIWZ oraz wzorze Umowy.
3. W cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia.
4. Zapoznaliśmy się z treścią SIWZ (w tym ze wzorem Umowy) i nie wnosimy do niej zastrzeżeń oraz przyjmujemy warunki w niej zawarte.
5. Uważamy się za związanych niniejszą ofertą na okres wskazany w SIWZ.
6. Wadium w wysokości **19 000,00 zł** (słownie: dziewiętnaście tysięcy złotych zero groszy) wnieśliśmy przed upływem terminu składania ofert.
7. Wadium wniesione w formie pieniądza należy zwrócić na rachunek bankowy nr .....prowadzony w banku .....
8. Zobowiązujemy się do wniesienia przed podpisaniem umowy zabezpieczenia należytego wykonania umowy w wysokości **10%** ceny całkowitej podanej w ofercie.

9. W przypadku przyznania nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.

10. Podwykonawcom zamierzamy powierzyć wykonanie następującej(-ych) części zamówienia (należy podać zakres prac oraz firmę Podwykonawcy):

a) .....

.....*

* w przypadku *niewypełnienia Zamawiający uzna, że Wykonawca nie zamierza powierzyć wykonania żadnej części zamówienia podwykonawcom.*

11. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na poniższy adres: .....

Dane kontaktowe: imię i nazwisko ....., nr tel. ....., adres e-mail: .....

12. Dokumenty wymienione od strony ..... do strony ..... stanowią tajemnicę przedsiębiorstwa i nie mogą być ujawnione pozostałym uczestnikom postępowania.

UWAGA:

Zamawiający przypomina, że stosownie do art. 8 ust. 3 ustawy Wykonawca winien nie później niż w terminie składania ofert wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.

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

* *rozporządzenie 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* oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2.*).*

** *w przypadku, gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie ma obowiązku składać (w takim przypadku Wykonawca może usunąć treści oświadczenia np. przez jego wykreślenie, przekreślenie, itp.).*

14. Jednocześnie zgodnie z treścią art. 91 ust. 3a ustawy oświadczam, że wybór przedmiotowej oferty:*

a) **nie będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego

b) **będzie** prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług

---

(należy wskazać: nazwę (rodzaj) towarów/usługi, których dostawa/świadczenie będzie prowadzić do jego powstania oraz wartość bez kwoty podatku od towarów i usług)

*) Niepotrzebne skreślić. W przypadku nie skreślenia (nie wskazania) żadnej z ww. treści oświadczenia i niewypełnienia powyższego pola oznaczonego: *„należy wskazać nazwę (rodzaj) towaru/usługi, których dostawa/świadczenie będzie prowadzić do jego powstania oraz ich wartość bez kwoty podatku od towarów i usług"* – Zamawiający uzna, że wybór przedmiotowej oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego.

15. Oferta została złożona na _____ stronach kolejno ponumerowanych od nr_____ do nr _____.

Świadom odpowiedzialności karnej oświadczam, że załączone do oferty dokumenty opisują stan prawny i faktyczny, aktualny na dzień złożenia oferty (art. 297 k.k.).