Wojewódzkie Wielospecjalistyczne Centrum Onkologii i Traumatologii
im. M. Kopernika w Łodzi
Dział Zamówień Publicznych
tel. 42 689 5819, 5911, faks 042 689 54 09
e-mail: przetargi@kopernik.lodz.pl

EZ.28.138. 2071 2022.AG

Łódź, dnia 02.11.2022 r.
Nr sprawy: **EZ.28.138.2022**

ODPOWIEDZI NA PYTANIA ORAZ ZMIANA TREŚCI SPECYFIKACJI WARUNKÓW ZAMÓWIENIA

Dotyczy: postępowanie o udzielenie zamówienia publicznego prowadzone w trybie przetargu nieograniczonego o wartości powyżej 215 000 Euro na **dostawę i wdrożenie sprzętu oraz oprogramowania podnoszącego poziom cyberbezpieczeństwa** dla Wojewódzkiego Wielospecjalistycznego Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi.

Zgodnie z dyspozycją art. 135 ust. 2 i 6 Ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (t.j. Dz.U. z 2022r. poz. 1710) przekazujemy Państwu odpowiedzi na pytania.

Pytanie nr 1
Czy zamawiający w Poz. 4 (w załączniku nr 2 stanowiącym OPZ) System odmiejscowienia kopii bezpieczeństwa - NAS 1 szt. wymaga dostarczenia urządzenia wraz z zainstalowanymi dyskami HDD? Jeżeli tak prosimy o określenie ilości i pojemności wymaganych dysków.

ODPOWIEDŹ: Tak, Zamawiający wymaga zainstalowanych dysków: 24 szt. x 16TB (wymagane dyski do pracy ciągłej). Zamawiający dokonuje stosownej modyfikacji załącznika nr 2 w tym zakresie.

Zamawiający na podstawie art. 137 ust. 1 i 2 Ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (t.j. Dz.U. z 2022r. poz. 1710) dokonuje zmiany treści SWZ i dokonaną zmianę udostępnia na stronie internetowej prowadzonego postępowania:

Zamawiający modyfikuje następujące załączniki:
Załącznik nr 2 –
ZESTAWIENIE PARAMETRÓW TECHNICZNYCH, WARUNKÓW GWARANCJI ORAZ SZKOLEŃ – PAKIET NR 1

POZOSTAŁE POSTANOWIENIA SPECYFIKACJI WARUNKÓW ZAMÓWIENIA POZOSTAJĄ BEZ ZMIAN

Z up. DYREKTORA
Wojewódzkiego Wielospecjalisty
Centrum Onkologii i Traumat
im. M. Kopernika w Łodzi
Z-CA DYREKTORA
ds. Ekonomiczno-Finansowych
GŁÓWNY KSIĘGOWY
mgr Agnieszka Kociszewska

SPECJALISTA
Dział Zamówień Publicznych
mgr Agnieszka Guzicka

Załącznik nr 2 do SWZ – zmiana z dnia 02.11.2022 r.
Nr sprawy EZ.28.138.2022

ZESTAWIENIE PARAMETRÓW TECHNICZNYCH I WARUNKÓW GWARANCJI

Dotyczy: postępowanie o udzielenie zamówienia publicznego prowadzone w trybie przetargu nieograniczonego o wartości powyżej 215 000 Euro na **dostawę i wdrożenie sprzętu oraz oprogramowania podnoszącego poziom cyberbezpieczeństwa** dla Wojewódzkiego Wielospecjalistycznego Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi.

Pakiet nr 1

Poz. 1 **System do analizy logów 1 szt. – Podać nazwę i producenta .....**				
Lp.	***Przedmiot zamówienia*** ***Wymagania minimalne Zamawiającego***	**Wartość graniczna parametru /parametr podlegający ocenie**	***PARAMETRY OFEROWANE: Potwierdzenie Wykonawcy wpisać: „TAK" lub opis parametrów oferowanych/ podać zakresy/ opisać***	**PUNKTACJA**
1.	Wymagania Ogólne W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie systemu linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).	**TAK/Podać**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

2.	Interfejsy, Dysk: System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.	**TAK/Podać**		**Bez oceny**
3.	Parametry wydajnościowe: 1. System musi być w stanie przyjmować minimum 10 GB logów na dzień. 2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.	**TAK**		**Bez oceny**
4.	W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje: Logowanie 1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: a. Listę najczęściej wykrywanych ataków. b. Listę najbardziej aktywnych użytkowników. c. Listę najczęściej wykorzystywanych aplikacji. d. Listę najczęściej odwiedzanych stron www. e. Listę krajów , do których nawiązywane są połączenia. f. Listę najczęściej wykorzystywanych polityk Firewall. g. Informacje o realizowanych połączeniach IPSec. 4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. 6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

5.	Raportowanie W zakresie raportowania system musi zapewniać: 1. Generowanie raportów co najmniej w formatach: PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Możliwość spolszczenia raportów. 4. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.	**TAK/Podać**		**Funkcja definiowania własnych raportów – 5 punktów**
6.	Korelacja logów W zakresie korelacji zdarzeń system musi zapewniać: 1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System musi korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe. 4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.	**TAK**		**Bez oceny**
7.	Zarządzanie 1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. 2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

8.	Serwisy i licencje 1. Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.	**TAK**		**Bez oceny**
9.	Instalacja i konfiguracja : • Uruchomienie systemu do analizy logów jako maszyny wirtualnej • Rekonfiguracja ustawień UTM i przekierowanie logów do systemu analizy logów • Customizacja ustawień serwera oraz kreowania raportów • Przeszkolenie 3 administratorów Zamawiającego z obsługi systemu	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

Poz. 2
System zabezpieczenia poczty email typu Antyspam 1 szt. – Podać nazwę i producenta .....

Lp.	*Przedmiot zamówienia* *Wymagania minimalne Zamawiającego*	**Wartość graniczna parametru /parametr podlegający ocenie**	***PARAMETRY OFEROWANE: Potwierdzenie Wykonawcy wpisać: „TAK" lub opis parametrów oferowanych/ podać zakresy/ opisać***	**PUNKTACJA**
1.	Wymagania ogólne System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systemu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów: 1. Tryb Gateway. 2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej). Parametry fizyczne systemu antyspamowego 1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 2 TB.	**TAK\Podać**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

2.	Ogólne funkcje systemu ochrony poczty Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje: 1. Wsparcie dla co najmniej 70 domen pocztowych. 2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 50 tys. wiadomości/godzinę. 3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all). 4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP. 5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości). 6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie. 7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. 8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. 9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP. 10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. 11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. 12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail. 13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. 14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. 15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. 16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. 17. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention). 18. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.	**TAK**		**Bez oceny**
3.	Kontrola antywirusowa i ochrona przed malware W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Skanowanie antywirusowe wiadomości SMTP. 2. Kwarantannę dla zainfekowanych plików. 3. Skanowanie załączników skompresowanych. 4. Blokowanie załączników w oparciu o typ pliku. 5. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antywirusowej. 6. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd	**TAK/Podać**		**Definiowanie komunikatów powiadomień w języku polskim – 5 punktów**

	zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu. 7. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. 8. Ochronę typu wirus outbrake. 9. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.			
4.	Kontrola antyspamowa System musi zapewniać poniższe funkcje i metody filtrowania spamu: 1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. 2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. 3. Szczegółowa kontrola nagłówka wiadomości. 4. Analiza Heurystyczna. 5. Współpraca z zewnętrznymi serwerami RBL, SURBL. 6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen. 7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników. 8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF. 9. Kontrola w oparciu o Greylisting oraz SPF. 10. Filtrowanie treści wiadomości i załączników. 11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. 12. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej. 13. Ochrona typu outbrake. 14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking). 15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata. 16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level) 17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.	**TAK**		**Bez oceny**
5.	Ochrona przed atakami na usługę poczty System musi zapewniać poniższe funkcje i metody filtrowania: 1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing). 2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. 3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

	4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing). 5. Weryfikacja poprawności adresu e-mail nadawcy.			
6.	Funkcje logowania i raportowania W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Logowanie do zewnętrznego serwera SYSLOG. 2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. 3. Logowanie informacji na temat spamu oraz niedozwolonych załączników. 4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. 5. Możliwość analizy przebiegu sesji SMTP. 6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. 7. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.	**TAK/Podać**		**Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu. – 5 punktów**
7.	Aktualizacje sygnatur, dostęp do bazy spamu W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. 2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.	**TAK**		**Bez oceny**
8.	Zarządzanie System ochrony poczty musi zapewniać poniższe funkcje: 1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. 2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy. 3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.	**TAK**		**Bez oceny**
9.	Certyfikaty Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji: 1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

10.	Serwisy i licencje System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: 1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 12 miesięcy.	**TAK**		**Bez oceny**
11.	Gwarancja oraz wsparcie 1. System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.	**TAK**		**Bez oceny**
12.	Instalacja i konfiguracja : • Wdrożenie maszyny do filtrowania treści email jako maszyna wirtualna • Uruchomienie oraz skonfigurowanie maszyny w trybie transparentnym • Dodanie oraz konfiguracja ochrony domeny Zamawiającego • Utworzenie polityk przychodzących jak i wychodzących • Hardening serwera • Przeszkolenie 3 administratorów Zamawiającego z obsługi systemu	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

Poz. 3
System odmiejscowienia kopii bezpieczeństwa - LTO 1 szt. – Podać nazwę i producenta .....

Lp.	*Przedmiot zamówienia* *Wymagania minimalne Zamawiającego*	**Wartość graniczna parametru /parametr podlegający ocenie**	***PARAMETRY OFEROWANE: Potwierdzenie Wykonawcy wpisać: „TAK" lub opis parametrów oferowanych/ podać zakresy/ opisać***	**PUNKTACJA**
1.	Wykorzystana technologia: LTO-8 Ultrium wspierające technologię partycjonowania nośników. Urządzenie musi mieć możliwość instalowania w tej samej obudowie i w tym samym czasie także napędów LTO szóstej, siódmej i dziewiątej generacji	**TAK**		**Bez oceny**
2.	Wbudowane napędy: Dwa napędy LTO-8 wyposażone w złącze z interfejsem FC 8GB. Urządzenie powinno mieć możliwość instalowania w tej samej obudowie i w tym samym czasie także napędów LTO z interfejsem dual SAS 6Gb oraz wspierać technologię LTFS (Linear Tape File System) umożliwiającą kopiowanie danych na taśmę bez konieczności użycia oprogramowania do backupu kompatybilną z systemami Linux, MAC OS i Microsoft. Prędkość zapisu pojedynczego napędu LTO-8 bez kompresji – minimum 300 MB/sek. Zainstalowane napędy powinny mieć możliwość dynamicznego i płynnego dopasowania prędkości do napływających danych (speed matching) w przedziale od 100 do 300 MB/sek. oraz stosować szyfrowanie danych metodą AES 256-bit	**TAK**		**Bez oceny**
3.	Ilość slotów i magazynki: Minimum 24 kieszenie na taśmy (urządzenie musi być dostarczone z kompletem magazynków). Jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów i magazynków zainstalowanych w urządzeniu. Wymagana ilość mail slot (I/E): min. 1. Wymiana taśm przez MailSlot powinna odbywać się bez konieczności wysuwania całego magazynka.	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

4.	Pojemność Pojemność bez kompresji – minimum 288TB	**TAK**		**Bez oceny**
5.	Obudowa Typu rack 19". Wszystkie elementy do montażu winny być dostarczone wraz z urządzeniem, wysokość maksymalnie 2U	**TAK**		**Bez oceny**
6.	Zarządzanie Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalne przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu FastEthernet. Wymagane wsparcie SNTP, protokołów SSL/TLS i IPv6 oraz definiowanie minimum 4 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, PenDrive. Operacja powinna być możliwa zarówna poprzez web GUI jak i poprzez panel kontrolny urządzenia. Wymagana możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI.	**TAK**		**Bez oceny**
7.	Dodatkowe interfejsy Biblioteka musi być wyposażone w interfejs sieciowy, interfejs USB oraz interfejs ADI	**TAK**		**Bez oceny**
8.	Obsługa urządzenia Wymagana możliwość wymiany napędów, zasilacza, modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Możliwość wyjmowania magazynków z urządzenia nawet przy braku zasilania. Zarówno napędy jak i zasilacz oraz moduł portów zarządzania powinny być wyposażone w lamki kontrolne, informujące o stanie technicznym i widoczne na tylnej stronie biblioteki.	**TAK**		**Bez oceny**
9.	Partycjonowanie Wymagane stworzenie 2 logicznych partycji – jeżeli do tej operacji konieczna jest dodatkowa licencja, należy ją dostarczyć wraz z urządzeniem	**TAK**		**Bez oceny**
10.	Wyposażenie Urządzenie musi być standardowo wyposażone w czytnik kodów kreskowych, zestaw kabli koniecznych do podłączenia do odpowiedniego kontrolera serwera umożliwiającego komunikację z urządzeniem – długość kabli min. 5m. Wraz z urządzeniem należy dostarczyć także zestaw nośników danych o pojemności bez kompresji minimum 12,0 TB każdy w ilości odpowiadającej ilości wszystkich dostępnych slotów na nośniki w dostarczonym urządzeniu plus dodatkowe 24 sztuki wraz z 2 nośnikami czyszczącymi, przy czym wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem, co należy potwierdzić odpowiednim oświadczeniem producenta urządzenia lub autoryzowanego dystrybutora urządzenia – wszystkie nośniki muszą być wyposażone w naklejki z kodami kreskowymi. Instrukcja instalacji - w języku polskim lub angielskim	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

11.	Gwarancja i oświadczenia 36 miesięcy w miejscu instalacji urządzenia z czasem reakcji na zgłoszenia do 4 godzin. Czas przyjmowania zgłoszeń serwisowych w trybie 24x7. Przystąpienie do fizycznej naprawy najpóźniej w następnym dniu roboczym od zgłoszenia awarii z terminem naprawy najpóźniej do 48 godzin od rozpoczęcia naprawy. Zgłaszania awarii wyłącznie poprzez ogólnopolską linię telefoniczną producenta lub autoryzowany serwis producenta posiadający certyfikat ISO9001 na usługi serwisowe – kontakt z serwisem wyłącznie w języku polskim. Oferowane urządzenie musi być zgodne z zapisami specyfikacji technicznej przetargu oraz zgodne z europejskimi normami dotyczącymi CE i WEEE. Wymaga się, aby wdrożenie i konfigurację urządzenia przeprowadziła osoba posiadająca certyfikat techniczny producenta urządzenia wystawiony w roku wdrożenia systemu.	**TAK/Podać**		**Gwarantowana możliwość rozszerzenia oferowanego serwisu do 84 miesięcy – 5 punktów**
12.	Instalacja i konfiguracja : • Instalacja we wskazanej szafie rack • Podłączenie do infrastruktury SAN • Konfiguracja stref przełączników SAN (QLOGIC SANbox 5802 FC) • Dodanie do istniejącego systemu kopii zapasowych (Commvault) • Konfiguracja min. 3 polityk systemu kopii zapasowych zgodnie z wymaganiami Zamawiającego. • Konfiguracja separacji danych zabezpieczająca przez atakami typu ransomware (ang. air gap) . Zamawiający zapewni serwer na którym możliwe będzie skonfigurowanie separacji (ang. air gap) • Testy wykonywania odseparowanych kopii bezpieczeństwa z wykorzystaniem mechanizmów air gap.	**TAK**		**Bez oceny**

Poz. 4
System odmiejscowienia kopii bezpieczeństwa - NAS 1 szt. – Podać nazwę i producenta .....

Lp.	*Przedmiot zamówienia* *Wymagania minimalne Zamawiającego*	**Wartość graniczna parametru /parametr podlegający ocenie**	***PARAMETRY OFEROWANE: Potwierdzenie Wykonawcy wpisać: „TAK" lub opis parametrów oferowanych/ podać zakresy/ opisać***	**PUNKTACJA**
1.	Procesor Min. 4,4 GHz 8 corowy	**TAK**		**Bez oceny**
2.	Architektura procesora 64-bit x86	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

3.	Pamięć RAM 32GB UDIMM DDR4	**TAK**		**Bez oceny**
4.	Pojemność maksymalna pamięci RAM Możliwość zainstalowania pamięci 64GB Min. 2 sloty wolne	**TAK/Podać**		**Możliwość zainstalowania pamięci 64GB – 0 punktów** **Możliwość zainstalowania pamięci 128GB – 4 punkty**
5.	Slot pamięci 4 x UDIMM DDR	**TAK**		**Bez oceny**
6.	Pamięć FLASH 5GB	**TAK**		**Bez oceny**
7.	Dyski: 24szt. x 16TB (wymagane dyski do pracy ciągłej) Wnęki dyskowe 24 x 3.5 cala SATA 6Gb/s, 3Gb/s	**TAK**		**Bez oceny**
8.	Kompatybilność dysków • 3,5-calowe dyski twarde SATA • 2,5-calowe dyski twarde SATA • 2,5-calowe dyski SSD SATA	**TAK**		**Bez oceny**
9.	Wymiana dysku podczas pracy • HOT-SWAP (Wymieniany podczas pracy)	**TAK**		**Bez oceny**
10.	Porty • 2 x Gigabit Ethernet Port (RJ45) • 1 x 10GbE SFP+ • 4 x USB 3.2 Gen 1 port • 1 x Type-C USB 3.2 Gen 2 10Gbps • 1 x Type-A USB 3.2 Gen 2 10Gbps	**TAK/Podać**		**1 x 10GbE SFP+ - 0 punktów** **2 x 10GbE SFP+ - 5 punktów**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

11.	Wskaźniki LED LAN, HDD	**TAK**		**Bez oceny**
12.	Przyciski Włącznik zasilania, Reset	**TAK**		**Bez oceny**
13.	Zasilanie 800W (x2), 100-240V	**TAK**		**Bez oceny**
14.	Obudowa 4U dedykowana do instalacji w szafie RACK	**TAK**		**Bez oceny**
15.	System ostrzegania Dźwiękowy	**TAK**		**Bez oceny**
16.	RAID Możliwość obsługi RAID:0,1,5,10,50,60	**TAK**		**Bez oceny**
17.	Gwarancja • 3 lata na serwer NAS - gwarancja producenta serwera NAS • 3 lata na zainstalowane dyski - gwarancja producenta dysków	**TAK**		**Bez oceny**
18.	Instalacja i konfiguracja : • Instalacja we wskazanej szafie rack • Podłączenie do infrastruktury SAN • Konfiguracja stref przełączników SAN (QLOGIC SANbox 5802 FC) • Dodanie do istniejącego systemu kopii zapasowych (Commvault) • Konfiguracja min. 3 polityk systemu kopii zapasowych zgodnie z wymaganiami Zamawiającego. • Konfiguracja separacji danych zabezpieczająca przez atakami typu ransomware (ang. air gap) . Zamawiający zapewni serwer na którym możliwe będzie skonfigurowanie separacji (ang. air gap) • Testy wykonywania odseparowanych kopii bezpieczeństwa z wykorzystaniem mechanizmów air gap.	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

Poz. 5 System odmiejscowienia kopii bezpieczeństwa – pakiet serwisowy 1 szt. – Podać nazwę i producenta				
Lp.	*Przedmiot zamówienia* *Wymagania minimalne Zamawiającego*	**Wartość graniczna parametru /parametr podlegający ocenie**	***PARAMETRY OFEROWANE: Potwierdzenie Wykonawcy wpisać: „TAK" lub opis parametrów oferowanych/ podać zakresy/ opisać***	**PUNKTACJA**
1.	Zapewnienie 24 miesięcy gwarancji producenta na posiadane macierze Fujitsu ETERNUS DX200 S4 [4601715058] , Fujitsu ETERNUS DX200 S4 [4601724441] w trybie on-site z gwarantowaną naprawą do końca następnego dnia roboczego od zgłoszenia. Zamawiający nie dopuszcza świadczenia gwarancji na macierz, półki i dyski przez serwis inny niż producenta posiadanej macierzy. Nie dopuszcza się również świadczenia gwarancji przez serwis nie posiadający autoryzacji producenta posiadanej macierzy. Uszkodzone dyski pozostają u Zamawiającego. Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego. System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół. Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta. W ramach pakietu serwisowego wymagana jest : - Aktualizacja posiadanej macierzy dyskowej Fujitsu ETERNUS DX200 S4 [4601715058] do najnowszego udostępnionego przez producenta Firmware. - Aktualizacja posiadanej macierzy dyskowej Fujitsu ETERNUS DX200 S4 [4601724441] do najnowszego udostępnionego przez producenta Firmware.	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

Poz. 6
System prewencji, reakcji i detekcji zagrożeń cyberbezpieczeństwa 1 szt. – Podać nazwę i producenta
.....

Lp.	*Przedmiot zamówienia* *Wymagania minimalne Zamawiającego*	**Wartość graniczna parametru /parametr podlegający ocenie**	***PARAMETRY OFEROWANE: Potwierdzenie Wykonawcy wpisać: „TAK" lub opis parametrów oferowanych/ podać zakresy/ opisać***	**PUNKTACJA**
1.	Zamawiający posiada nieobjęty wsparciem i niezaktualizowany system składający się z licencji : SolarWinds Network Performance Monitor SLX (unlimited elements-Standard Polling Throughput) SolarWinds NetFlow Traffic Analyzer for SolarWinds NPM SLX SolarWinds Network Configuration Manager DL200 (up to 200 nodes) SolarWinds User Device Tracker UT10000 (up to 10000 ports) SolarWinds Server & Application Monitor ALX (unlimited monitors-Standard Polling Throughput) SolarWinds Security Event Manager (formerly LEM)- SEM250 (up to 250 nodes) SolarWinds Virtualization Manager VM64 (up to 64 sockets) SolarWinds Network Topology Mapper Wymaga się zakup i wdrożenie licencji umożliwiających aktualizację produktu do najnowszej wersji Orion Platform wersja 2022.2 wraz z utrzymania wsparcia produktu na okres min. 12 miesięcy (nowe funkcje i poprawki błędów) Bezpośredni dostęp do aktualizacji oprogramowania w okresie wsparcia. Dostępu do wsparcia producenta w trybie 24x7 W okresie wsparcia pełna subskrypcja na zajęcia prowadzone przez instruktorów SolarWinds Academy	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

Poz. 7
Skaner podatności 1 szt. – Podać nazwę i producenta .....

Lp.	*Przedmiot zamówienia* *Wymagania minimalne Zamawiającego*	**Wartość graniczna parametru /parametr podlegający ocenie**	***PARAMETRY OFEROWANE: Potwierdzenie Wykonawcy wpisać: „TAK" lub opis parametrów oferowanych/ podać zakresy/ opisać***	**PUNKTACJA**
1.	Musi być zarządzany przez przeglądarkę, zabrania się używania jakiegokolwiek grubego agenta	**TAK/Podać**		**Możliwość wymuszenia polityki haseł dla administratorów logujących się do systemu – 6 punktów**
2.	musi mieć opcję dostarczenia jako oprogramowanie i maszyna wirtualna. W przypadku dostarczenia jako maszyna wirtualna muszą być wspierane środowiska Hyper-V oraz Vmware. W przypadku systemu operacyjnego na którym będzie instalowany produkt jako oprogramowanie, muszą być wpierane co najmniej systemy operacyjne: Ubuntu 14.04/16.04, SUSE Enterprise 11 SP4/12, Windows Server 2012/ 2012 R2/2016/2019/2022, Windows 7 SP1,8.1,10,11 (32 bit), CentOS 7/8, Oracle Linux 6/7/8, macOS 10.10 – 10.15,11.x	**TAK**		**Bez oceny**
3.	licencja nie może być ograniczona ilością skanowanych adresów IP,	**TAK**		**Bez oceny**
4.	system musi mieć możliwość pracy bez dostępu do Internetu, a dostarczanie nowych reguł skanowania musi odbywać się za pomocą ręcznej aktualizacji z poziomu interfejsu,	**TAK**		**Bez oceny**
5.	interfejs systemu musi przedstawiać informacje o systemie takie jak użycie CPU, pamięci, ilość skanowanych systemów, ilość sesji TCP, ruch przesyłany i odbierany do/z skanera,	**TAK**		**Bez oceny**
6.	musi być dostarczony z predefiniowanymi politykami skanowania minimum polityka dotycząca wykrycia hostów w sieci, WannaCry, Log4Shell, SoloriGate	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

7.	musi być możliwość skanowania systemów pod kontem zgodności z regulacjami takimi jak CIS, DISA. W przypadku zgodności z regulacjami, producent musi dostarczać gotowe wzorce polityk zgodności z CIS, DISA jak również musi być możliwość zbudowania własnej polityki sprawdzania pod kontem zgodności z przyjętymi regulacjami w firmie w oparciu o dokumentację dostarczoną przez producenta. Wzorce zgodności z regulacjami dostarczone przez producenta muszą być możliwe do edycji. Sprawdzanie systemu pod kontem zgodności z regulacjami oraz dostęp do wzorców regulacji na stronie producenta nie wymaga żadnej dodatkowej licencji,	**TAK**		**Bez oceny**
8.	musi być możliwość tworzenia własnej polityki skanowania w której administrator wybiera jakie podatności będą sprawdzane	**TAK**		**Bez oceny**
9.	system musi umożliwiać skanowanie z uwierzytelnieniem i bez uwierzytelnienia. W przypadku skanowania z uwierzytelnieniem muszą być wspierane następujące metody: - Windows – Kerberos, LM Hash, NTLM Hash, hasło - SSH – kluczy publiczny, Kerberos, hasło, certyfikat, - SNMP3	**TAK**		**Bez oceny**
10.	w przypadku skanowania systemów opartych o system linux/unix musi być możliwość podniesienia uprawnień przynajmniej za pomocą poniższych technik: .k5login, Cisco (enable), dzdo, pbrun, su, sudo	**TAK**		**Bez oceny**
11.	system pozwala na tworzenie jak również używanie dostarczonych przez producenta wzorców skanowania pod kontem konfiguracji systemów bezpieczeństwa i sieciowych. Muszą być wspierane przynajmniej wymienione systemy: FireEye, SonicWall, Fortinet FortiGate, BlueCoat ProxySG, Amazon AWS, Microsoft Azure	**TAK**		**Bez oceny**
12.	system zezwala na tworzenie harmonogramu skanowania podatności jak również uruchomienia na żądanie,	**TAK**		**Bez oceny**
13.	system musi pozwalać na porównanie wyników dwóch wykonanych skanów	**TAK**		**Bez oceny**
14.	system musi umożliwiać sprawdzenie konfiguracji systemu bez dostępu do niego. Sprawdzenie ma być dokonana na podstawie pliku konfiguracyjnego. Muszą być wspierane przynajmniej systemy jak: FireEye, SonicWall ,Fortinet FortiGate, BlueCoat ProxySG,	**TAK**		**Bez oceny**
15.	system musi umożliwiać filtrowanie wyników przynajmniej po takich parametrach jak: CVE, CVSS , CVSS v3/v2, Czy jest dostępny exploit, hostname, kiedy była upubliczniona aktualizacja na dana podatność, port, protokół, wrażliwość w oparciu o punktację CVSS, zwartość opisu podatności, Bugtraq ID, CERT Vulnerability ID, CPE, IAVB ID,	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

16.	system musi być wspierany przez dodatkowy system punktowania podatności prezentowany w GUI oparty min. o uczenie maszynowe i aktualizowany codziennie. Mechanizm ten wspierany musi być również przez zespół ludzi producenta skanera, którzy analizują wyniki z modelu uczenia maszynowego jak również monitorują źródła takie jak min. Darknet,	**TAK**		**Bez oceny**
17.	możliwość wyeksportowania wyników skanowania przynajmniej do formatów HTML, CSV, PDF	**TAK/Podać**		**system musi mieć możliwość przetrzymywania historii wykonanych skanów – 5 punktów**
18.	możliwość wygenerowania przynajmniej raportu Top 10 Podatności, Wykryty system operacyjny, nie wpierane oprogramowanie, Podatności na które są znane exploity	**TAK**		**Bez oceny**
19.	możliwość dodania nazwy oraz własnego logo do raportu	**TAK**		**Bez oceny**
20.	system musi prezentować wynik skanowania wraz z rekomendacją od jakich aktualizacji zacząć, aby wyeliminować największe ryzyko przez daną aktualizację	**TAK**		**Bez oceny**
21.	system musi umożliwiać zmianę wrażliwości wykrytej podatności w wyniku wykonanego skanu, musi być możliwość ukrycia w wynikach danej podatności	**TAK**		**Bez oceny**
22.	system musi umożliwiać zmianę elementu wykrywającego daną podatność zawężając regułę do konkretnego systemu skanowanego oraz czas jak długo dana reguła ma obowiązywać	**TAK**		**Bez oceny**
23.	aktualizacja reguł wykrywania podatności musi być wykonywana automatycznie w przypadku dostępu systemu do Internetu	**TAK**		**Bez oceny**
24.	system musi umożliwiać automatyczną instalację Terrascan z poziomu GUI skanera	**TAK**		**Bez oceny**
25.	system musi umożliwiać nagrywanie ruchu pomiędzy skanerem, a skanowanym hostem w przypadku rozwiązywania problemów	**TAK**		**Bez oceny**
26.	system musi pozwalać na ustawienie skanowania adresów IP w przypadkowej kolejności	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

27.	system musi umożliwiać ustawienia dotyczące wydajności skanowania tzn. liczba jednocześnie skanowanych systemów, liczba jednoczesnych elementów sprawdzanych na skanowanym systemie, maksymalna liczba jednoczesnych sesji TCP na skanowany system oraz maksymalna liczba jednoczesnych sesji na skan	**TAK**		**Bez oceny**
28.	system musi umożliwiać wykonanie w ramach jednego skanu skanowania pod kontem podatności oraz zgodności z regulacjami	**TAK**		**Bez oceny**
29.	• Wdrożenie skanera podatności w postaci maszyny wirtualnej OnPremise z roczną licencją bez limitów hostów czy ilości skanowań • Licencja musi umożliwiać na aktualizację bazy sygnatur w czasie rzeczywistym • Maszyna musi informować w czasie rzeczywistym o zmianie statusu podatności • Maszyna musi posiadać możliwość tworzenia wzorców własnych raportów bezpieczeństwa • Maszyna musi posiadać minimum 60 000 wpisów w bazie sygnatur opartej na CVE • Maszyna musi spierać wykrywanie podatności tak zwanych zero-day • Maszyna musi posiadać sygnatury obejmujące urządzenia sieciowe, urządzenie peryferyjne, urządzenia mobilne, system operacyjne oraz systemy wirtualizacje. • Szkolenie dla min. 3 administratorów Zamawiającego, z zakresu: - przeprowadzania skanów podatności - tworzenia własnej polityki skanowania - eksportowania wyników skanowania - konfiguracji powiadomień o wynikach skanowania	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

Załącznik nr 2 do SWZ
Nr sprawy EZ.28.138.2022

ZESTAWIENIE PARAMETRÓW TECHNICZNYCH I WARUNKÓW GWARANCJI

Dotyczy: postępowanie o udzielenie zamówienia publicznego prowadzone w trybie przetargu nieograniczonego o wartości powyżej 215 000 Euro na **dostawę i wdrożenie sprzętu oraz oprogramowania podnoszącego poziom cyberbezpieczeństwa** dla Wojewódzkiego Wielospecjalistycznego Centrum Onkologii i Traumatologii im. M. Kopernika w Łodzi.

Pakiet nr 2

Poz. 1 **System zabezpieczenia sieci typu UTM 1 szt. – Podać nazwę i producenta .....**				
Lp.	***Przedmiot zamówienia*** ***Wymagania minimalne Zamawiającego***	**Wartość graniczna parametru /parametr podlegający ocenie**	***PARAMETRY OFEROWANE: Potwierdzenie Wykonawcy wpisać: „TAK"*** ***lub opis parametrów oferowanych/ podać zakresy/ opisać***	**PUNKTACJA**
1.	Wymagania Ogólne System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

	System wspiera protokoły IPv4 oraz IPv6 w zakresie: •Firewall. •Ochrony w warstwie aplikacji. •Protokołów routingu dynamicznego			
2.	Redundancja, monitoring i wykrywanie awarii 1.W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2.Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3.Monitoring stanu realizowanych połączeń VPN. 4.System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. 5.System ma pracować w postaci redundantnego klastra.	**TAK**		**Bez oceny**
3.	Interfejsy, Dysk, Zasilanie: 1.System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: •10 portami Gigabit Ethernet RJ-45. •8 gniazdami SFP 1 Gbps. •2 gniazdami SFP+ 10 Gbps. 2.System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3.System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie 1x AC.	**TAK/Podać**		**System jest wyposażony w zasilanie 1x AC. – 0 punktów** **System jest wyposażony w zasilanie 2x AC. – 15 punktów**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

4.	Parametry wydajnościowe: 1. W zakresie Firewall'a obsługa nie mniej niż 8 mln. jednoczesnych połączeń oraz 450 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 35 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 14.5 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 20 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 9.5 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 6.5 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 7.8 Gbps.	**TAK**		**Bez oceny**
5.	Funkcje Systemu Bezpieczeństwa: W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

6.	Polityki, Firewall 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.	**TAK**		**Bez oceny**
7.	Połączenia VPN 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności	**TAK**		**Bez oceny**

	automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.			
8.	Routing i obsługa łączy WAN W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.	**TAK**		**Bez oceny**
9.	Funkcje SD-WAN 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).	**TAK**		**Bez oceny**
10.	Zarządzanie pasmem 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

	4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.			
11.	Ochrona przed malware 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.	**TAK**		**Bez oceny**
12.	Ochrona przed atakami 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej.	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

	Mechanizmy ochrony IPS nie mogą działać globalnie.			
13.	Kontrola aplikacji 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).	**TAK**		**Bez oceny**
14.	Kontrola WWW 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana	**TAK**		**Bez oceny**

	inspekcja szyfrowanej komunikacji.			
15.	Uwierzytelnianie użytkowników w ramach sesji 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.	**TAK**		**Bez oceny**
16.	Zarządzanie 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

17.	Logowanie 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. System zapewnia możliwość logowania do serwera SYSLOG. 5. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.	**TAK/Podać**		**Możliwość włączenia logowania per reguła w polityce firewall. - 10 punktów**
18.	Certyfikaty Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.	**TAK**		**Bez oceny**
19.	Testy wydajnościowe oraz funkcjonalne Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.	**TAK**		**Bez oceny**
20.	Serwisy i licencje Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.	**TAK**		**Bez oceny**
21.	Gwarancja oraz wsparcie 1. System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

22.	Instalacja i konfiguracja : •Wdrożenie klastra wysokiej dostępności klastra UTM zgodnie z wymaganiami zamawiającego •Zabezpieczenie punktu styku z siecią Internet; •Uruchomienie sond IDS/IPS •Uruchomienie blokowania niebezpiecznych aplikacji •Uruchomienie filtrowania dostępu do stron WWW •Rekonfiguracja trasowania w sieci LAN •Rekonfiguracja- migracja ustawień serwera DHCP, DNS; •Zabezpieczenie serwera DNS, DHCP; •Utworzenie nowych polityk kontroli dostępu •Oparcie segmentacji sieci na UTM - migracja ustawień z przełączników warstwy core oraz dystrybucyjnej •Opracowanie powdrożeniowej dokumentacji technicznej	**TAK**		**Bez oceny**

Poz. 2 **Przełącznik sieci SAN 4 szt. – Podać nazwę i producenta .....**				
Lp.	***Przedmiot zamówienia*** ***Wymagania minimalne Zamawiającego***	**Wartość graniczna parametru /parametr podlegający ocenie**	***PARAMETRY OFEROWANE: Potwierdzenie Wykonawcy wpisać: „TAK"*** ***lub opis parametrów oferowanych/ podać zakresy/ opisać***	**PUNKTACJA**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

1.	Ilość portów FC: Łączna ilość aktywnych portów FC – 24 z możliwością rozszerzenia do 64 szt. 32Gb/s portów Fibre Channel. Rozbudowa nie może odbywać się poprzez zakup dodatkowych, modułów sprzętowych, jedynie poprzez zakup licencji. (z wyłączeniem modułów SFP/SFP+ i kabli) W pełni rozbudowany przełącznik nie może zajmować w szafie RACK więcej niż 1U.	**TAK**		**Bez oceny**
2.	Przepustowość portu: Porty uniwersalne o przepustowości 32Gbit/s, z obsługą przepustowości 4Gbit/s, 8Gbit/s i 16 Gbit/s (w zależności od rodzaju zastosowanych wkładek SFP). z automatycznym wyborem przepustowości (auto-sensing), obsługa trybu full-duplex dla wszystkich wspieranych przepustowości. Zagregowana przepustowość dla maksymalnej obsady portów minimum 2Tbit/s	**TAK**		**Bez oceny**
3.	Interfejsy optyczne: Moduły do transmisji światłowodowej z prędkością min. 32Gbit/s poprzez kabel światłowodowy wielomodowy (Short-Wavelenght) z interfejsem LC, liczba modułów dostosowana do liczby aktywnych portów, możliwość pracy z prędkością 8Gbit/s/16 Gbit/s/32Gb/s	**TAK**		**Bez oceny**
4.	Inne funkcje i wyposażenie: 1.Obsługa trybów pracy portów FC: D_Port, E_port, EX_port, F_port, N-Port, AE_Port. 2.Obsługa funkcji PoD (Ports on Demand) przydziału licencji dla aktywnych portów FC 3.Aktywne licencje : a)Webtools, b)Zoning, 4.Możliwość zdalnej aktualizacji firmware'u switcha 5.Dedykowany interfejs RJ-45 min 10/100/1000 Mb/s do zarządzania poprzez sieć Ethernet 6.Możliwość zarzadzania typu in-band poporzez Fibre Channel, 7.Dedykowany interfejs RJ-45 lub DB9 do zarządzania poprzez interfejs szeregowy, dedykowany port USB umożliwiający upgrade FW i zapis logów 8.Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

	9.Dedykowany interfejs RJ-45 min 10/100/1000 Mb/s do zarządzania poprzez sieć Ethernet 10.Możliwość zarzadzania typu in-band poporzez Fibre Channel, 11.Dedykowany interfejs RJ-45 lub DB9 do zarządzania poprzez interfejs szeregowy, dedykowany port USB umożliwiający upgrade FW i zapis logów 12.Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia 13.Zarządzanie poprzez przeglądarkę WWW z obsługą połączeń szyfrowanych min. 128-bit SSL oraz poprzez usługę SSH 14.Zarządzanie poprzez konsole znakową tzw. CLI 15.Wsparcie dla protokołu SNMP v.3 16.Ilość buforów ramek minimum 15.000 17.Możliwość obsługi funkcjonalności (funkcjonalności poniższe sa opcjonalne, nie sa wymagane do zaoferowania w oferowanej konfiguracji) : a)FullFabric (z obsługą do min. 239 przełączników FC) b)FabricWatch, Trunking, Adaptive Networking, Access Gateway c)Advanced Performance Monitoring d)Inter Switch Link (ISL) z przepustowością maks. 256 Gb/s /ISL			
5.	Montowany w szafie typu rack 19"	**TAK**		**Bez oceny**
6.	Typ obudowy: Wysokość przełącznika 1U w systemie montażu w szafie typu rack 19".	**TAK**		**Bez oceny**
7.	1.Zasilanie z sieci prądu przemiennego o napięciu w zakresie 90- 264V/50-60Hz V, maksymalny pobór mocy podczas pracy urządzenia 205W (dla obsady wszystkich 64-ch portów). 2.Dwa Redundantne zasilacze z możliwością wymiany na gorąco. 3.Wentylatory nadmiarowe zintegrowane w zasilaczach	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym

8.	Zasilanie/chłodzenie: 1.Zasilanie z sieci prądu przemiennego o napięciu w zakresie 90- 264V/50-60Hz V, maksymalny pobór mocy podczas pracy urządzenia 205W (dla obsady wszystkich 64-ch portów). 2.Jeden zasilacz. 3.Wentylatory nadmiarowe zintegrowane w zasilaczu/zasilaczach	**TAK/Podać**		**Jeden zasilacz – 0 punktów** **Dwa Redundantne zasilacze z możliwością wymiany na gorąco. – 15 punktów**
9.	Gwarancja/dostawa: Przełącznik musi być dostarczony przez producenta serwera i musi posiadać jego gwarancję i serwis. Urządzenie musi być objęte gwarancją producenta na okres 3 lata z naprawą wykonywaną w miejscu instalacji urządzenia	**TAK**		**Bez oceny**
10.	Instalacja i konfiguracja : • Instalacja we wskazanej szafie rack • Konfiguracja stref dostarczanych przełączników SAN • Migracja infrastruktury SAN z 4 posiadanych przełączników QLOGIC SANbox 5802 FC na dostarczone przełączniki SAN • Migracja nie może powodować przerw w pracy środowiska aplikacyjnego Zamawiającego.	**TAK**		**Bez oceny**

Formularz należy podpisać kwalifikowanym podpisem elektronicznym