Samodzielny Publiczny
Zespół Zakładów Opieki Zdrowotnej w Glinojecku
ul. Targowa 6, 06-450 Glinojeck

tel./fax 23 674 00 31 e-mail: spzzozglinojeck@e-glinojeck.pl

Załącznik nr 1 do zapytania ofertowego .

Opis Przedmiotu Zamówienia

Dotyczący zamówienia przeprowadzanego zgodnie z zasadą konkurencyjności określoną w Wytycznych z dnia 22 sierpnia 2019r. w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego oraz Funduszu Spójności na lata 2014-2020
dla projektu pn: **„Wdrożenie e-usług w placówce POZ" nr POIS.11.03.00-00-0074/22 , finansowanego ze środków Programu Operacyjnego Infrastruktura i Środowisko 2014-2020**

ZAMAWIAJĄCY

Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej w Glinojecku
06-450 Glinojeck, ul. Targowa 6
NIP-5661854776, REGON 130951714, KRS 0000180951

1. Ogólne informacje

Przedmiotem zamówienia jest: sprzęt teleinformatyczny, który umożliwi tworzenie i udostępnianie elektronicznej dokumentacji medycznej (EDM) oraz świadczenie e-usług.

Zamówienie składa się z poniższych pozycji:

1. **Serwer – 1 szt.**
2. **Oprogramowanie serwerowe – 1 szt 2 maszyny wirtualne**
3. **Licencje dostępowe CAL RDS– 10 szt.**
4. **Licencje dostępowe CAL - 25 szt**
5. **Oprogramowanie do wirtualizacji**
6. **Urządzenia sieciowe switch - 1 szt.**
7. **Urządzenia do tworzenia kopii zapasowych (serwer plików - 1 wraz z oprogramowaniem do tworzenia kopii bezpieczeństwa**
8. **Zasilacz awaryjny UPS**
9. **Instalacja i konfiguracja sprzętu IT oraz szkolenie Administratora Zamawiającego**
10. **Router UTM**

Kody CPV zamówienia:

32420000-3 Urządzenia sieciowe

31214100-0 Przełączniki

48821000-9 Serwery sieciowe

48823000-3 Serwery plików

51610000-1 Usługi instalowania urządzeń komputerowych i przetwarzania informacji

Wszystkie zaproponowane przez Wykonawcę sprzęty równoważne muszą:

a) posiadać parametry techniczne i funkcjonalne nie gorsze od określonych w Zapytaniu ofertowym,
b) posiadać stosowne certyfikaty, świadectwa dopuszczenia, atesty itp.

Wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) sprzętów lub normy, aprobaty, specyfikacje i systemy, Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych nie gorszych niż wymagane przez Zamawiającego w dokumentacji zapytania.

Zamawiający informuje, że w takiej sytuacji przedmiotowe zapisy są jedynie przykładowe i stanowią wskazanie dla Wykonawcy, jakie cechy powinny posiadać składniki użyte do realizacji przedmiotu zamówienia. Zamawiający, dopuszcza oferowanie sprzętów równoważnych. Urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie urządzeń, estetyka itp.), jakim muszą odpowiadać urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów/produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach.
Zamawiający dokonując zamówienia musi brać pod uwagę sytuację bieżąca tj. wymagania ściśle wymuszone przez System Dziedzinowy użytkowany przez Zamawiającego.
System Dziedzinowy przetestowano i obecnie pracuje na maszynach wirtualnych:

- Debian 1 maszyna wirtualna ,
- Windows Serwer 1 maszyna wirtualna – dwie maszyny wirtualne Hyper V: Windows Server 2016 Standard,
- Windows 10-1 maszyna wirtualna

Poza tym Zamawiający posiada:

- 25 licencji CAL na oprogramowanie w Windows Server 2016
- Remote Desktop Services w ilości 4 szt..
- Oracle 18C ASFU SE2 liczba procesorów max. 2

Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia, dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania

określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, uwiarygodniających te rozwiązania. Zmiana koncepcji pracy Systemy Dziedzinowego wymaga oddzielnych konsultacji.

Obecnie używany System Dziedzinowy to KS-SOMED KAMSOFT S.A.

.

Lp.	Nazwa produktu do zakupu	Ilość (szt.)	Min. okres gwarancji
1.	Serwer	1	36 miesięcy
2.	Oprogramowanie serwerowe – 1 szt.	2 maszyny wirtualne	Licencja bezterminowa
3.	Licencje dostępowe CAL RDS – 10 szt.	10	Licencja bezterminowa
4.	Urządzenia do tworzenia kopii zapasowych -serwer plików - 1 szt	1	Licencja bezterminowa
5	Switch	1	24 miesiące
6	Zasilacz awaryjny UPS	1	24 miesiące
7.	Instalacja i konfiguracja sprzętu IT	1	36 miesięcy
8	Router UTM	1	36 miesięcy
9	Licencje dostępowe CAL 25 szt		Licencja bezterminowa
10	Oprogramowanie do wirtualizacji		Licencja bezterminowa

2. Miejsce realizacji dostaw

Miejscem dostawy przedmiotu zamówienia jest miejsce realizacji projektu tj. Samodzielny Publiczny Zakłada Opieki Zdrowotnej w Glinojecku Targowa 6 .06-450 Glinojeck

3. Termin Wykonania Zamówienia

Przedmiot zamówienia musi być zrealizowany w nieprzekraczalnym terminie do 30 dni kalendarzowych od dnia podpisania umowy z Wykonawcą.

4. Minimalne parametry i opis techniczny.

CZĘŚĆ I

4.1. Serwer wraz z oprogramowaniem do wirtualizacji– 1 szt.

Minimalne wymagania techniczne i funkcjonalne przedstawiają się następująco:

Lp.	Parametr	Minimalne wymagania
1.	Typ procesora	o minimalnym taktowaniu 2,5 GHz
2.	Liczba procesorów	2 - warunek patrz uwaga dot. Oracle
3.	Pamięć systemowa	128 GB **DDR4-SDRAM**
4	Obsługiwane kontrolery RAID	Kontroler pamięci (RAID) - SATA 6Gb/s / SAS
5	**Zainstalowane dyski**	SSD SATA 6G 2TB 2 szt. HD SATA 6G 4TB 4 szt.
6	PCI	Gniazda PCI Express x8 (Gen 3.x) Gniazda PCI Express x16 (Gen 3.x)
7	Przewodowa sieć LAN	Tak
8	Sieć Zainstalowane karty	Port 2,5 Gigabit Ethernet (2,5G/1G/100M) 2 porty Port 10 Gigabit sfp+ sieci Ethernet 2 porty
Pozostałe minimalne parametry		
Zasilanie Max. 800 W Obsługa zasilania zapasowego (RPS) Ilość zainstalowanych, nadmiarowych źródeł zasilania 2 SZT Ilość portów USB 3.2 Gen 1 (3.1 Gen 1) Typu-A Liczba portów USB 2.0 Gniazda PCI Express x8 (Gen 3.x) Gniazda PCI Express x16 (Gen 3.x)		

Zdalna administracja Zintegrowany kontroler zdalnego dostępu z technologią kontrolera cyklu eksploatacji umożliwia administratorom monitorowanie, obsługę i aktualizowanie serwera oraz rozwiązywanie problemów i usuwanie skutków awarii niezależnie od ich umiejscowienia — bez zastosowania agentów. Kontroler działa niezależnie od systemu operacyjnego i stanu lub dostępności monitora maszyn wirtualnych. Rack (max. 2U) **szyny montażowe w zestawie** **Zgodność:** Microsoft Hyper-V Server 2022 Microsoft Windows Server 2022 Datacenter Microsoft Windows Server 2022 Standard Microsoft Windows Server 2022 Essentials Microsoft Windows Storage Server 2022 Microsoft Windows Storage Server 2012 R2 Standard VMware vSphere 6.5 VMware vSphere 6.0 SUSE Linux Enterprise Server 12 SUSE Linux Enterprise Server 11 Red Hat Enterprise Linux 7 Red Hat Enterprise Linux 6 Oracle Linux 7 A	
Gwarancja	36 m-cy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Uszkodzony dysk pozostaje u Zamawiającego
Stan sprzętu:	Nowy
Oprogramowanie do wirtualizacji specyfikacja techniczna	Maks. ilość hostów ESXi 3 Maks. ilość CPU/Host 2 Maks. ilość VM/Host 1024 Typ licencji Licencja wieczysta z prawem do aktualizacji vSphere Hypervisor TAK vCenter Server Essentials TAK vSphere VMFS TAK VMware vSphere vStorage APIs TAK

4.2. Oprogramowanie serwerowe systemowe – 1 szt. 2 maszyny wirtualne.

Minimalne wymagania techniczne i funkcjonalne przedstawiają się następująco:

Zgodnie z opisem Zamawiający posiada licencje dostępowe Windows Serwer 2022

Lp.	Parametr	Minimalne wymagania
1	Oprogramowanie serwerowe musi umożliwić uruchomienie oprogramowania dziedzinowego użytkowanego aktualnie u Zamawiającego oraz pełną współpracę z ActiveDirectory. Licencje zostaną wykorzystane do uruchomienia oprogramowana na nowym serwerze zakupionym w ramach niniejszego postępowania.	TAK
2	Licencja bez ograniczeń czasowych. Warunki licencjonowania muszą zezwalać na zmianę wersji systemu operacyjnego na niższą z zachowaniem wsparcia technicznego oraz na przeniesienie licencji systemu operacyjnego na inny fizyczny serwer	TAK
3	instalacja i użytkowanie aplikacji 32- i 64-bitowych na dostarczonym serwerowym systemie operacyjnym;	TAK
4	w ramach dostarczonej licencji zawarta możliwość instalacji oprogramowania na serwerze wieloprocesorowym;	TAK
5	obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych);	TAK
6	wielkość obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego – przynajmniej 4TB;	TAK
7	obsługa dostępu wielościeżkowego do zasobów LAN poprzez karty Gigabit Ethernet i szybsze, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu;	TAK
8	praca w roli klienta domeny Microsoft Active Directory;	TAK
9	zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2016;	TAK
10	zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP);	TAK
11	zawarta możliwość uruchomienia roli serwera DNS;	TAK
12	zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP);	TAK

13	zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;	TAK
14	zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;	TAK
15	zawarta funkcjonalność szyfrowania dysków;	TAK
16	dostępny hypervisor umożliwiający uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera;	TAK
17	w ramach licencji zawarte prawo do wirtualizacji dwóch systemów na zasobach sprzętowych serwera;	TAK
18	w ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego;	TAK
19	wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).	TAK

4.3. Licencje dostępowe RDS 10szt. , CAL – 25 szt.

Minimalne wymagania techniczne i funkcjonalne przedstawiają się następująco:

Lp.	Parametr	Minimalne wymagania
1.	Licencje RDS – Remote Desktop Services Windows Serwer 2022	10 szt

	Licencje dostępowe CAL Windows Serwer 2022	25 szt.
2	Licencja	Bezterminowa

4.4. Urządzenie sieciowe switch - 1 szt.

Minimalne wymagania techniczne i funkcjonalne przedstawiają się następująco:

4.4.1. Switch – 1 szt.

Lp.	Parametr	Minimalne wymagania
1	Typ zarządzania Zarządzanie sieciowe Liczba portów 17 25 GbE SFP28 16 10 GbE BASE-T (RJ45) 1 Gniazdo do zarządzania 1 port 1GbE RJ45 Informacje o zasilaniu Zasilacz wewnętrzny Maks. zużycie energii 80W Typ zasilania wejściowego AC Zakres napięcia wejściowego 100-240 VAC, 50/60 Hz Tabela adresów MAC 32K Łączna przepustowość nieblokująca 410Gbps Zdolność przełącznia 820Gbps Interfejs zarządzania Sieć Web Obsługiwane normy IEEE 802.3 Ethernet IEEE 802.3u 100BASE-T IEEE 802.3ab 1000BASE-T IEEE 802.3bz 2.5G/5GBase-T IEEE 802.3an 10G BASE-T IEEE 802.3z 1000BASE-SX/LX	

	IEEE 802.3ae 10G Fiber IEEE 802.3x Kontrola przepływu Full-Duplex IEEE 802.3by 25 Gigabit Ethernet IEEE 802.1Q VLAN Tagowanie IEEE 802.1w RSTP IEEE 802.3ad LACP IEEE 802.1AB LLDP IEEE 802.3az Energy Efficient Ethernet IEEE 802.1p Klasa usługi Certyfikaty CE, FCC, VCCI, BSMI Zgodność elektromagnetyczna Class Gwarancja od 24 miesiące
2	Stan sprzętu: Nowy

4.5. Urządzenia do tworzenia kopii zapasowych serwer plików wraz z oprogramowaniem backup - 1 szt.

Minimalne wymagania techniczne i funkcjonalne przedstawiają się następująco:

1	Procesor	Czterordzeniowy wbudowany procesor o taktowaniu 2,2 GHz
2	Architektura procesora	64-bitowy x86
3	Koprocesor arytmetyczny FPU	
4	Mechanizm szyfrowania	(AES-NI)
5	Pamięć systemowa	8 GB UDIMM DDR4 (1 x 8 GB)
6	Maksymalna pojemność pamięci	64 GB (2 x 32 GB)
7	Gniazdo pamięci	2 x Long-DIMM DDR4 Support ECC memory
8	Pamięć flash	5 GB (ochrona systemu operacyjnego przed podwójnym rozruchem)
9	Wnęka dysków	12 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s
10	Kompatybilność dysków	3,5-calowe dyski twarde SATA 2,5-calowe dyski twarde SATA 2,5-calowe dyski SSD SATA
11	Sieć	Port 2,5 Gigabit Ethernet (2,5G/1G/100M)

		Dodatkowo zainstalowana karta sieciowa sztuk 1 - 2x10GbE sfp+
12	Rack **szyny montażowe w zestawie**	
13	HDD	**Zamontowane dyski HDD 4TB 8 sztuk – gwarancja dysków 5 lat.** Zoptymalizowany i zgodny do pracy w serwerach plików. Uszkodzony dysk pozostaje u Zamawiającego
14	Stan sprzętu:	Nowy

Minimalne wymagania techniczne i funkcjonalne dla oprogramowania backup przedstawiają się następująco:

Wsparcie i uaktualnienia	3 lata
Kompatybilność	Windows, Linux jako VA lub AMI QNAP NAS
Backup	VMware Backup Hyper-V Backup Backup to Cloud (AWS, Azure)
Odzyskiwanie plików	Natychmiastowe odzyskanie VM Dla programu Microsoft® Exchange Dla programu Microsoft® SQL Dla programu Microsoft® Active Directory
Odzyskiwanie po awarii	Replikacja VMware Replikacja Hyper-V Odzyskiwanie VM
Zmniejszenie przestrzeni	Globalna wymiana danych Pomiń pliki i partycję SWAP
Wsparcie	Wsparcie aplikacji i bazy danych Weryfikacja Screenshot Echange Log Truncation SQL Log Truncation Szyfrowanie
Wydajność	Transfer danych bez użycia sieci LAN Przyśpieszenie sieci Bezpośredni dostęp do sieci SAN Pełne przechowywanie danych syntetycznych
Pozostałe funkcje	• **wsparcie dla najnowszych wersji systemów wirtualizacji** – Microsoft Hyper-V 2022 oraz VMware vSphere 6.5

	• licencjonowanie per gniazdo fizycznego procesora • kompresja i deduplikacja w obrębie całego repozytorium backupu • łatwe wyszukiwanie i kasowanie niepotrzebnych backupów • weryfikacja backupu i migawek • ochrona kontenera • pomijanie plików tymczasowych i pliku wymiany • szyfrowanie przy użyciu AES256bit • replikacja backupu • przywracanie na poziomie plików

4.6. Zasilacz awaryjny UPS – 1 szt.

Lp.	Parametr	Minimalne wymagania
1	Zasilacz awaryjny UPS 2200VA/2700W, topologia Line-interactive	
2	Gwarancja	24 miesiące
3	Stan sprzętu:	Nowy

4.7. Instalacja i konfiguracja sprzętu IT

Minimalne wymagania przedstawiają się następująco:

Lp.	Parametr
1.	1. Fizyczny montaż i podłączeniem wszystkich zakupionych urządzeń 2. Fizyczny montaż urządzeń serwerowych we wskazanym przez Zamawiającego miejscu. 3. Instalacja wirtualnej infrastruktury opartej na maszynach wirtualnych 4. Instalacja dostarczonego systemu Windows Serwer w stworzonej infrastrukturze maszyn wirtualnych. 5. Instalacja i konfiguracja maszyny wirtualnej – serwera do zbierania logów z bramy UTM 6. Instalacja i konfiguracja maszyny wirtualnej - serwera dla środowiska do wykonywania kopii zapasowych w oparciu o oprogramowanie dostarczone przez zamawiającego 7. Wdrożenie polityk backupowych w środowisku Zamawiającego

	8. Zaprojektowanie w współpracy z Zamawiającym harmonogramu wykonywania kopii, z uwzględnieniem środowiska Zamawiającego. 9. Instalację oprogramowania w środowisku Zamawiającego. 10. Implementację harmonogramu wykonywania kopii w zainstalowanym oprogramowaniu. 11. Wykonanie testowych kopii, wraz z weryfikacją poprawności ich wykonania. 12. Testy odtworzenia danych środowiska. 13. Konfiguracja oprogramowanie do wykonywania kopii zapasowych do obsługi macierzy dyskowych NAS oraz wdrożenie polityk backupowych w uwzględniających kopie zapasowe na te macierze. 14. Uczestnictwo we wdrożeniu wszystkich usług Zamawiającego, które będą wymagały konsultacji z dostawcą urządzenia – współpraca z dostawcami 15. Instalacja i konfiguracja maszyny wirtualnej – serwera do zbierania logów z bramy UTM 16. usługa szkolenia Administratora SPZZOZ Glinojeck w zakresie technologii oraz zastosowanych narzędzi 17. Opieka Inżynierska w ramach uruchomionych urządzeń i narzędzi – 1 rok.

CZĘŚĆ II

1. Router UTM

Lp.	Parametr	Minimalne wymagania
1	**Wymagania Ogólne** **firewall (hardware) 4000 Mbit/s** **Przepustowość Firewall: 4000 Mbit/s** **Przepustowość VPN: 2500 Mbit/s** **Wydajność SSL: 200 transkacji/s** **Wydajność HTTP: 2500 transkacji/s** **Certyfikaty: FCC Part 15B, Class B, CE, RCM, VCCI, UL/cUL, CB, BSMI ICSA Labs:** **Firewall, IPsec, IPS, Antivirus, SSL-VPN** 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. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. **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. **Interfejsy, Dysk, Zasilanie:** 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 10 portami Gigabit Ethernet RJ-45. • 2 gniazdami SFP 1 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 AC. **Parametry wydajnościowe:** 1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 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 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.

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).

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.

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 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.

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.

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).

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.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

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.

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. Mechanizmy ochrony IPS nie mogą działać globalnie.

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).

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 inspekcja szyfrowanej komunikacji.

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.

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.

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. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Certyfikaty

Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

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 36 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 36 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.

Rozszerzone wsparcie serwisowe AHB/SOS

System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy.

System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:

- Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
- Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
- Doradztwo w zakresie konfiguracji.
- Zdalne wsparcie techniczne.
- Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
- Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
- Przygotowanie urządzenia do zdalnej konfiguracji.
- Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
- Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
- Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
- Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

	Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym. • Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego. **Opisy do wymagań ogólnych** 1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.
2	Stan sprzętu: Nowy
3	Usługa instalacji obejmuje: • fizyczny montaż sprzętu, • uruchomienie zapisu logów dostępnych do analizy dla Zamawiającego. • konfiguracja urządzenie na potrzeby SPZZOZ Glinojeck zgodnie z zasadą dobrych praktyk i aktualnych wymagań prawnych dotyczących bezpieczeństwa • konfiguracja połączeń VPN pomiędzy jednostkami podległymi a instytucją macierzystą, liczba jednostek podległych filii 2 szt. • instalacja i konfiguracja polis bezpieczeństwa dla 25 stacji roboczych • uczestnictwo we wdrożeniu wszystkich usług Zamawiającego, które będą wymagały konsultacji z dostawcą urządzenia UTM – współpraca z dostawcami

	• usługa szkolenia Administratora SPZZOZ Glinojeck w zakresie technologii oraz zastosowanych narzędzi.