Załącznik nr.4 do zapytania ofertowego

Opis Przedmiotu Zamówienia

1. Serwer aplikacyjny - 1kpl

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. serwera o wysokiej wydajności i elastyczności, przeznaczonego do instalacji w GOPS Bolesław.

Wymagania:

1. Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji min. 4 dysków SAS/SATA 2,5" lub 3,5".
2. Serwer wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz możliwością instalacji przedniego panelu zamykanego na klucz, chroniącego dyski przed nieuprawnionym wyjęciem.
3. Płyta główna dedykowana serwerowa, wyprodukowana i zaprojektowana przez producenta serwera.
4. Chipset dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych.
5. Zainstalowany jeden procesor min. 6-rdzeniowy o taktowaniu min. 3.1GHz (base frequency) umożliwiający osiągnięcie w teście PassMark – CPU Mark wyniku dla jednego procesora min. 18 500 pkt. Testy dla oferowanego modelu procesora muszą być opublikowane i ogólnie dostępne na stronie: https://www.cpubenchmark.net/high_end_cpus.html
6. Pamięć RAM min. 32 GB RAM DDR4 RDIMM 3200MT/s, w modułach po 16 GB RAM.
7. Na płycie głównej powinny znajdować się minimum 4 sloty przeznaczone do instalacji pamięci RAM. możliwość rozbudowy do min 128GB.
8. Wbudowane porty:
    a. Min. 5 portów USB z czego nie mniej niż 1 port USB 3.0 i USB TYP-C na przednim panelu obudowy, 2 porty USB 3.0 na tylnym panelu obudowy oraz 2 porty USB 3.0 na płycie głównej.
    b. Złącze USB TYP-C na przednim panelu musi umożliwiać dostęp do modułu zarządzania serwerem przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android lub iOS.
    c. 1 port VGA na tylnym panelu obudowy.
    d. Powyższe porty USB, USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
9. Min. 1 aktywny slot PCI-E 4.0 x16
10. Zainstalowane i w pełni funkcjonalne interfejsy:
    a. min. 1 port RJ-45 Ethernet management port,
    b. min. 4 porty 1Gb/s Ethernet w standardzie BaseT,
    c. Porty nie mogą zajmować slotów PCI-E
11. Zainstalowany sprzętowy kontroler RAID umożliwiający skonfigurowanie poziomów RAID 0, 1, 10.. Kontroler powinien posiadać wsparcie dla dysków SAS i SATA.
12. Pamięć masowa: zainstalowane 4 dyski serwerowe SSD o pojemności min. 960 GB każdy.

13. Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo.
14. Ilość zainstalowanych wentylatorów musi umożliwiać wydajne chłodzenie dla maksymalnej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).
15. Min. dwa identyczne zasilacze o mocy min. 800W o sprawności min 92% zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera.
16. Bezpieczeństwo:
    a. Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.
    b. Moduł TPM 2.0.
17. Możliwość wyposażenia serwera w panel diagnostyczny (LCD) umieszczony z przodu obudowy serwera, umożliwiający:
    a. wyświetlenie podstawowych informacji o serwerze, w tym numer seryjny oraz wersja oprogramowania zarządzającego i BIOS
    b. wyświetlanie stanu i logów, dla pamięci RAM, procesorów, pamięci masowej, wentylatorów, czujników temperatury i zasilaczy
    c. przywracanie konta administratora
    d. wyświetlanie w czasie rzeczywistym temperatury wlotu powietrza do serwera
    e. wyświetlanie w czasie rzeczywistym temperatury procesorów
    f. konfigurowanie ustawień sieciowych modułu zarządzania.
18. Karta Zarządzania niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port 1 Gigabit Ethernet RJ-45 (1000Mbps) i umożliwiająca:
    a. monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.),
    b. monitorowanie w czasie rzeczywistym poboru prądu przez serwer,
    c. zbieranie logów błędów hardware,
    d. przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury,
    e. montowanie wirtualnych napędów,
    f. zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego,
    g. wysyłanie zawiadomień droga mailową i poprzez SNMP
    h. wsparcia dla IPMI, SSH, Redfish
    i. wparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows,
    j. nadawanie ról użytkownikom,
    k. możliwość wykonania aktualizacji oprogramowania do zarządzania serwerem, BIOS, zasilaczy, LCD,
    l. możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem.
19. Wraz ze serwerem dostarczone powinno być oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na:
    a. włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejęcie pełnej konsoli graficznej serwerów.
    b. tworzenie szablonów instalacyjnych dla systemów operacyjnych.

c. tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów.
d. zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera.
e. aktualizacja sterowników i BIOS serwerów.
f. zbieranie statystyk zużycia energii dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych.

20. Zgodność z normą ISO 9001 oraz ISO 14001 lub równoważnymi.
21. Serwer musi posiadać deklaracja CE.
22. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów, Microsoft Windows Server 2022. Certyfikat lub inny dokument potwierdzający zgodność z dostarczanym systemem operacyjnym należy dołączyć do oferty.
23. Razem z serwerem należy dostarczyć Windows Server 2022 Essentials lub równoważny.
24. Razem z serwerem należy dostarczyć 10 licencji dostępowych na użytkownika jeśli oprogramowanie systemu operacyjnego takich licencji wymaga.
25. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
26. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego serwera i oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta.
27. Gwarancja:
    a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP.
    b. Urządzenie objęte minimum 36 miesięcznym okresem gwarancji w trybie onsite z gwarantowanym czasem reakcji najpóźniej Next Business Day godziny od momentu zgłoszenia usterki.
    c. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
    d. Usługi gwarancyjne świadczone przez autoryzowanego partnera serwisowego producenta/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny.
    e. Wymagane oświadczenie producenta oferowanego serwera, że wymagany poziom serwisu z wymaganym SLA został zaoferowany na potrzeby oferty w niniejszym postępowaniu.
    f. Wymaganie oświadczenie producenta potwierdzające, że elementy, z których zbudowany jest serwer, są produktami producenta tych serwerów lub są przez niego certyfikowane oraz całe są objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA.
    g. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
        i. możliwość pobierania najnowszego firmware,
        ii. dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
        iii. dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,
        iv. otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.

28. Zakres prac wdrożeniowych:
    a. Analiza przedwdrożeniowa:
        i. Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
        ii. Opracowanie planu wdrożenia.
    b. Wdrożenie i konfiguracja:
        i. Instalacja serwera wraz z oprogramowaniem.
        ii. Konfiguracja serwera i oprogramowania zgodnie z wymaganiami zamawiającego.
        iii. Integracja z istniejącymi systemami IT zamawiającego.
    c. Testy akceptacyjne:
        i. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
        ii. Weryfikacja poprawności działania serwera oraz oprogramowania.

2. Serwer NAS – 1 kpl

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. serwera NAS przeznaczonego do instalacji w GOPS Bolesław.

Cecha użytkowa	minimalne parametry techniczne i użytkowe
Typ	Sieciowy serwer plików NAS do montażu w szafie typu rack.
Obudowa	• przystosowana do montażu w szafie rack 19”; • maksymalna wielkość 2U; • min. 8s zt gniazd na dyski twarde 2,5’ i 3,5”; HDD/SSD • szyny do montażu w szafie 19”;
Procesor	Min. 4 fizycznych rdzeni Procesor musi osiągać w teście wydajności PassMark PerformanceTest co najmniej 5400 punktów Passmark CPU Multithread Rating Mark (wynik dostępny pod adresem: http://www.cpubenchmark.net).
Pamięć RAM	Min. 4 GB DDR4 ECC z możliwością rozbudowy do min. 32GB. Rodzaj pamięci SODIMM DDR4
Dyski twarde typ 1	8 szt. identycznych dysków 2) pojemność każdego dysku min. 12TB; 3) prędkość obrotowa min. 7200 rpm; 4) interfejs SATA 6Gb/s;
Kontroler pamięci masowej	1) obsługiwane tryby raid: min. 0,1,5,6,10 JBOD; 2) obsługiwane typy dysków: SATA;

Zasilacze	• Min. 2 szt. wentylatory , 100 - 240 V (prąd zmienny) • 50 / 60 Hz, jednofazowo
Interfejs sieciowy	• Min.4 x 10/100/1000 Mbit/s • Możliwość rozszerzenia w karte 10/25 GbE SFP+
Gniazda we/wy	• 1 x eSATA • 4 x RJ-45 LAN • 2 x USB 3.0 Uwaga: Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, rozgałęziaczy, przejściówek, itp
Gniazdo rozszerzeń	Min 1 x PCIe 3.0 x 8
System operacyjny - funkcje	• Obsługa autoryzacji Windows AD i LDAP; • Kompatybilność ze środowiskami wirtualizacyjnymi Vmware vSphere, Microsoft Hyper-V • . Obsługa protokołów SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP)
Certyfikaty i standardy	1) Certyfikat ISO9001 dla producenta sprzętu 2) deklaracja zgodności CE.
Warunki gwarancji – serwer	• min. 3 lata gwarancji producenta na części i robociznę, naprawa w miejscu użytkowania, reakcja serwisowa w następnym dniu roboczym od zgłoszenia awarii; • serwis urządzenia musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta
Warunki gwarancji – dyski twarde	1) min. 5 lat gwarancji producenta na części i robociznę; 2) W przypadku awarii dyski twarde pozostają u Zamawiającego

3. System do wykonywania kopi zapasowych

Przedmiotem zamówienia jest dostawa, konfiguracja i uruchomienie oprogramowania do wykonywania kopii zapasowych w GOPS Bolesław oraz przeszkolenie administratorów po stronie zamawiającego . Wymagana jest dożywotnia licencja dla dostarczonego systemu archiwizacji (backupu) danych.

Wymagane funkcjonalności które muszą być realizowane przez dostarczony system:

- Możliwość backupu min 10 komputerów, 2 serwerów, oraz 2 hostów wirtualizacji.
- Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich
- Program serwerowy kompatybilny z systemami: Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology
- Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology
- Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików)
- Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)
- Automatyczny backup przy wyłączaniu komputera
- Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ?
- Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)
- Backup baz danych i plików poczty w trybie online i offline
- Kopie rotacyjne (wersjonowanie)
- Zapis archiwów w otwartym formacie (ZIP 64-bit)
- Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi
- Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)
- Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej
- Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych
- Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO
- Kompresja po stronie stacji roboczej

- Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP,
- Replikcacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows)
- Centralne sterowanie całym Systemem z jednego miejsca
- Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników
- Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN
- Wysyłanie Alertów administracyjnych na e-mail
- Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych
- Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki
- Automatyczna aktualizacja oprogramowania na komputerach zdalnych
- Bezterminowa licencja - licencja nie może być ograniczona czasowo
- Interfejs, instrukcja i pomoc techniczna w języku polskim
- Wsparcie techniczne przez okres min. 12 miesięcy od daty uruchomienia.

4. Przełącznik dostępowy – 1 szt.

Przedmiotem zamówienia jest dostawa, konfiguracja i uruchomienie przełącznika dostępowego w GOPS Bolesław

	minimalne parametry techniczne i użytkowe
1.	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. Oprogramowanie (firmware) dostarczony przez producenta urządzenia.
2.	Wymagane parametry fizyczne: a) możliwość montażu w stelażu/szafie 19” b) wysokość maksymalna 1U c) głębokość bez zainstalowanego zasilacza nie większa niż 35 cm d) minimum jeden zasilacz 230V AC e) zakres temperatur pracy ciągłej co najmniej od 0°C do +45 °C f) zakres wilgotności pracy co najmniej 5% - 90%

3.	Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie: ● 24 porty 100/1000BASE-T zgodne ze standardem 802.3at (minimalny budżet mocy PoE: 370W) ● 4 porty 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 1G-SX, 1G-LX, 1GBase-T (RJ45), kabli DAC Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
4.	Przełącznik musi posiadać następujące porty służące do zarządzania: ● Port konsoli. Zamawiający dopuszcza port konsoli ze złączem Micro-USB lub port konsoli RS232 ze złączem RJ45
5.	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: a) Zarządzanie stosem poprzez jeden adres IP b) Do min. 9 jednostek w stosie c) Porty do stackowania mogą być współdzielone z portami typu uplink. d) Magistrala stackująca o wydajności minimum 80Gb/s e) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation) f) Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree g) Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia. h) W stosie musi być możliwość budowania stosu pomiędzy przełącznikami: TYP1, TYP2, TYP3, TYP4 W ramach postępowania Zamawiający wymaga dostarczenia oryginalnego kabla producenta do stackowania o długości min 1m.
6.	Układ przełączający o wydajności min. 128 Gbps, wydajność przełączania przynajmniej 95 Mpps
7.	Obsługa min. 32 500 adresów MAC
8.	Wbudowana pamięć RAM min. 1GB. Procesor wielordzeniowy. Minimalne taktowanie procesora 1000MHz
9.	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512MB
10.	Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
11.	Możliwość skonfigurowania min. 32 interfejsów vlan interface SVI działających równocześnie

12.	Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad
13.	Obsługa minimum 120 grup LAG
14.	Obsługa ramek jumbo o wielkości min. 9216 bajtów
15.	Obsługa sFlow
16.	Wsparcie dla G.8032 ERPS
17.	Obsługa protokołu VRRP
18.	Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP). Wsparcie dla mechanizmu PVST+.
19.	Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng, IS-IS, BGP. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania
20.	Obsługa min. 6 100 tras dla routingu IPv4
21.	Obsługa min. 2 000 tras dla routingu IPv6 Obsługa min. 2 020 IPv6 neighbor discovery (ND)
22.	Obsługa protokołów związanych z obsługą ruchu typu multicast: a) IGMP v1, v2 i v3 b) IGMP Snooping v2 i v3 c) PIM-SM, PIM-SSM i PIM-DM d) MSDP i MLD Snooping e) minimum 2000 tras multicast dla IPv4 i minimum 1000 tras multicast dla IPv6
23.	Minimalny rozmiar tablicy ARP 4 092 wpisów
24.	Obsługa protokołów LLDP i LLDP-MED
25.	Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client
26.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: a) min. 3 poziomy dostępu administracyjnego poprzez konsolę b) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL c) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC d) obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 1500 reguł ACL e) zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2 f) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP

	g) obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard h) możliwość synchronizacji czasu zgodnie z NTP lub SNTP
27.	Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach: a) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP b) wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ
28.	Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA).
29.	Wymagane opcje zarządzania: a) możliwość lokalnej obserwacji ruchu na określonym porcie b) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC) c) wsparcie dla skyptów python uruchamianych na urządzeniu d) wsparcie dla RMON
30.	Wraz z urządzeniami muszą zostać dostarczone: a) pełna dokumentacja w języku polskim lub angielskim b) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana
31.	Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
32.	Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
33.	Zamawiający wymaga, aby urządzenia posiadały 3-letni serwis gwarancyjny świadczony przez Wykonawcę lub autoryzowany serwis producenta. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki). Usługa serwisu musi być świadczona w języku polskim. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.

34.	Wraz z urządzeniem należy dostarczyć systemu centralnego zarządzania pochodzący od producenta oferowanych urządzeń. System centralnego zarządzania może być dostarczony w formie: 1) Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej Lub 2) Dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego. Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego. W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych. System centralnego zarządzania musi umożliwiać: - tworzenie VLANów - ustawianie trybu pracy danego portu (access/trunk) z dodaniem odpowiedniego VLANu - tworzenie połączeń zagregowanych - monitorowanie statusu pracy przełącznika i portów - możliwość uruchomienia CLI przełącznika w panelu systemu do zarządzania - możliwość wykonania aktualizacji oprogramowania dla danego przełącznika sieciowego

5. Zasilacz awaryjny (UPS) – 1 szt.

Przedmiotem zamówienia jest dostawa i uruchomienie UPS w GOPS Bolesław.

cecha techniczno-funkcjonalna	minimalne parametry techniczne i użytkowe
Technologia	VFI (true on-line, podwójne przetwarzanie energii)
Moc znamionowa	3kVA / 2,7kW
Wyjściowy współczynnik mocy (PF)	0,9
Wejściowy współczynnik mocy	cosϕ ≥ 0,99
Napięcie wejściowe	208/220/230/240 VAC + N
Tolerancja napięcia wejściowego	176 – 300 VAC
Częstotliwość wejściowa	40-70 Hz
Minimalna sprawność AC-AC w trybie pracy on-line z obciążeniem 100%	≥92%

Minimalna sprawność w trybie ECO	≥97,0% dla 100% obciążenia
Napięcie wyjściowe	208/220/230/240 VAC
Częstotliwość wyjściowa	50/60Hz (programowalna)
Czas podtrzymania	5 minut
Intuicyjny panel graficzny	Wymagane
Stabilizacja napięcia wyjściowego	±1%
Zniekształcenia napięcia wyjściowego	≤ 2% z obciążeniem liniowym ≤ 5% z obciążeniem nieliniowym
Współczynnik szczytu przy obciążeniu znamionowym	3:1
Przeciążenie inwertera	105%-125% przez 1 minutę 125% -150% przez 30 sekund >150% przez 300 milisekund
Złącze interfejsów	RS232 + USB
Interfejs EPO (do wyłącznika ppoż.)	Wymagane
Wbudowana karta sieciowa SNMP	Wymagane, jedna karta pozwalająca na komunikację poprzez protokoły: SNMP, Modbus TCP/IP, Modbus RTU
Możliwość pracy jako konwerter częstotliwości	Wymagane
Baterie	Szczelne, bezobsługowe, w technologii AGM o żywotności projektowanej minimum 5 lat w temperaturze 25 stopni Celsjusza
Możliwość zainstalowania akumulatorów wewnątrz modułu zasilacza UPS (bez konieczności użycia modułu bateryjnego)	Wymagane
Test bateryjny	Wymagane
Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego	Wymagane
Poziom hałasu w odległości 1m	≤ 50 dBA
Rejestr zdarzeń	Wymagane
Spełnienie wszystkich obowiązujących norm bezpieczeństwa potwierdzone deklaracją zgodności CE	Wymagane

Maks. wymiary modułu UPS (szer. x gł. x wys.)	440 x 560 x 88 mm (2U)
Gwarancja	Min. 24 miesiące

6. UTM - 2 kpl

Przedmiotem zamówienia jest dostawa , konfiguracja i uruchomienie urządzenia UTM w GOPS Bolesław oraz UG Bolesław.

6.1 Opis wymagań techniczno-funkcjonalnych UTM dla GOPS Bolesław – 1 kpl

Funkcje modułu Firewall dla jednostki podległej GOPS Typ 1

1. Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
2. Możliwość uruchomienia w formie klastra wysokiej dostępności (HA) - co najmniej Active-Passive.
3. Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
4. Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.
5. Musi obsługiwać Multicast routing.
6. Musi obsługiwać Policy Based routing.
7. Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.
8. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
9. Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.
10. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
11. Musi obsługiwać Dynamic DNS.
12. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
13. Musi obsługiwać translację portów: PAT.
14. Musi obsługiwać IPSec NAT traversal.
15. Musi obsługiwać mechanizm Policy Based NAT.
16. Musi obsługiwać VLAN 802.1Q.
17. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
18. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
19. Musi mieć możliwość obsługi zapasowego łącza typu 4G LTE/5G poprzez podłączenie zewnętrznego modemu USB.
20. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
21. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.
22. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza, minimum dla wartości: utrata pakietów, opóźnienie, jitter.
23. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
24. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.

25. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.
26. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.
27. Musi posiadać co najmniej dwie metody transparentnej autoryzacji nie wymagające instalacji dedykowanego agenta na stacjach roboczych użytkowników.
28. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.
29. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
30. Musi dostarczać mechanizm identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
31. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
32. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
33. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.
34. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
35. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.
36. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.
37. Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
38. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.
39. Musi ochraniać przed minimum: atakami DoS, pofragmentowanymi i zniekształconymi pakietami, zagrożeniami mieszanymi (Blended threats).
40. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.
41. VPN site-to-site musi wspierać minimum: IKEv2, IPSec, tunele oparte na politykach i routingu, TLS hub and spoke.
42. VPN client-to-site musi wspierać minimum: IKEv2, IPSec, L2TP, TLS

Specyfikacja UTM:

1. Firewall musi zapewnić obsługę na poziomie minimalnym:
   3.14 Gbps dla pracy w trybie firewall,
   403 Mbps dla pracy w trybie full scan (włączone mechanizmy bezpieczeństwa takie jak: AV, IPS)
2. Ilość obsługiwanych sieci VLAN: 10
3. Firewall musi obsługiwać 1 300 000 jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną 16 000 połączeń na sekundę.
4. Minimalna ilość portów 10/100/1000 BaseT: 5
5. Wsparcie połączeń VPN site-to-site lub client-to-site dla minimum 10 użytkowników.

Dostarczony system bezpieczeństwa (UTM) musi zapewniać:

1. Ochronę z wykorzystaniem mechanizmów IPS.
2. Ochronę antywirusową.

3. Ochronę przed niechcianą pocztą.
4. Kontrolę wykorzystywanych aplikacji.
5. Możliwość filtrowania URL.

W ramach ochrony przed atakami system musi zapewniać:

1. Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 8000 definicji sygnatur.
2. Automatyczne blokowanie znanych źródeł ataków.
3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).
5. Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer OverFlow, Remote File Inclusions.
6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.

W ramach kontroli antywirusowej system musi zapewniać:

1. Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie
2. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.
3. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.
4. Możliwość skanowania plików o rozmiarze co najmniej 10MB.
5. Możliwość zdefiniowania rozmiaru skanowanego pliku.
6. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
7. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
8. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.
9. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.

W ramach kontroli antyspamowej system musi zapewniać:

1. Analizę wiadomości pocztowych w oparciu o technologię Recurrent Pattern Detection.
2. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.
3. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
4. Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
5. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.

W ramach filtrowania zawartości URL system musi zapewniać:

1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
2. Baza filtra url powinna zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
3. Odpytywanie bazy on-line w czasie rzeczywistym.
4. Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym, dlaczego dostęp do strony www został zablokowany.
5. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
6. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
7. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.

8. Możliwość określenia różnego rodzaju akcji dla połączeń do wybranych adresów URL na podstawie reputacji.
9. Możliwość filtrowania treści w oparciu o typy MIME.
10. Możliwość blokowania plików cookies dla określonych domen.
11. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
12. Analizę treści dla protokołu https.
13. Wyłączenie inspekcji https dla wybranych kategorii stron www.

W ramach kontroli aplikacyjnej system musi zapewniać:

1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
2. Ilość rozpoznawanych aplikacji: nie mniej niż 1000, podzielonych na kategorie.
3. W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
4. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.

Wymagane funkcje VPN systemu:

1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
5. Obsługa Dead Peer Detection (DPD).
6. Wsparcie dla IKEv1 i IKEv2.
7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.
10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.
12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.

Zarządzanie:

1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.

6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.
8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.

Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania:

1. Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
2. Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
3. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
4. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline
5. Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
6. Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
7. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
8. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
9. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
10. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
11. Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
12. Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
13. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
14. Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
15. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
16. System ma mieć możliwość generowania raportów w formacie PDF oraz opcję eksportowania szczegółowych informacji do pliku CSV.
17. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
18. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
19. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
20. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
21. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
22. Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.

6.2 Opis wymagań techniczno-funkcjonalnych UTM dla UG Bolesław – 1 kpl

Funkcje modułu Firewall dla jednostki Urząd Gminy Typ 2

1.Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
2.Możliwość uruchomienia w formie klastra wysokiej dostępności (HA) - co najmniej Active-Passive.
3.Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
4.Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.
5.Musi obsługiwać Multicast routing.
6.Musi obsługiwać Policy Based routing.
7.Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code

Point) w ramach zapewnienia jakości usług.

7. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
8. Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.
9. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
10. Musi obsługiwać Dynamic DNS.
11. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
12. Musi obsługiwać translację portów: PAT.
13. Musi obsługiwać IPSec NAT traversal.
14. Musi obsługiwać mechanizm Policy Based NAT.
15. Musi obsługiwać VLAN 802.1Q.
16. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
17. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
18. Musi mieć możliwość obsługi zapasowego łącza typu 4G LTE/5G poprzez podłączenie zewnętrznego modemu USB.
19. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
20. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.
21. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza, minimum dla wartości: utrata pakietów, opóźnienie, jitter.
22. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
23. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
24. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.
25. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.
26. Musi posiadać co najmniej dwie metody transparentnej autoryzacji nie wymagające instalacji dedykowanego agenta na stacjach roboczych użytkowników.
27. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.
28. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
29. Musi dostarczać mechanizm identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
30. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
31. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
32. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.
33. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
34. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.
35. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.
36. Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
37. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.
38. Musi ochraniać przed minimum: atakami DoS, pofragmentowanymi i zniekształconymi pakietami, zagrożeniami mieszanymi (Blended threats).

39. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.
40. VPN site-to-site musi wspierać minimum: IKEv2, IPSec, tunele oparte na politykach i routingu, TLS hub and spoke.
41. VPN client-to-site musi wspierać minimum: IKEv2, IPSec, L2TP, TLS

Specyfikacja UTM:

1.Firewall musi zapewnić obsługę na poziomie minimalnym:

- 3.94 Gbps dla pracy w trybie firewall
- 557 Mbps dla pracy w trybie full scan (włączone mechanizmy bezpieczeństwa takie jak: AV, IPS)

2.Ilość obsługiwanych sieci VLAN: 50

3.Firewall musi obsługiwać 3 850 000 jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną 26 500 połączeń na sekundę.

4.Minimalna ilość portów 10/100/1000 BaseT: 5

5.Wsparcie połączeń VPN site-to-site lub client-to-site dla minimum 30 użytkowników.

Dostarczony system bezpieczeństwa (UTM) musi zapewniać:

1. Ochronę z wykorzystaniem mechanizmów IPS.
2. Ochronę antywirusową.
3. Ochronę przed niechcianą pocztą.
4. Kontrolę wykorzystywanych aplikacji.
5. Możliwość filtrowania URL.

W ramach ochrony przed atakami system musi zapewniać:

1. Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 8000 definicji sygnatur.
2. Automatyczne blokowanie znanych źródeł ataków.
3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).
5. Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer OverFlow, Remote File Inclusions.
6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.

W ramach kontroli antywirusowej system musi zapewniać:

1. Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie
2. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.
3. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.
4. Możliwość skanowania plików o rozmiarze co najmniej 10MB.
5. Możliwość zdefiniowania rozmiaru skanowanego pliku.
6. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
7. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
8. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.
9. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.

W ramach kontroli antyspamowej system musi zapewniać:

1. Analizę wiadomości pocztowych w oparciu o technologię Recurrent Pattern Detection.
2. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.
3. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
4. Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
5. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.

W ramach filtrowania zawartości URL system musi zapewniać:

1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
2. Baza filtra url powinna zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
3. Odpytywanie bazy on-line w czasie rzeczywistym.
4. Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym, dlaczego dostęp do strony www został zablokowany.
5. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
6. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
7. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.
8. Możliwość określenia różnego rodzaju akcji dla połączeń do wybranych adresów URL na podstawie reputacji.
9. Możliwość filtrowania treści w oparciu o typy MIME.
10. Możliwość blokowania plików cookies dla określonych domen.
11. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
12. Analizę treści dla protokołu https.
13. Wyłączenie inspekcji https dla wybranych kategorii stron www.

W ramach kontroli aplikacyjnej system musi zapewniać:

1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
2. Ilość rozpoznawanych aplikacji: nie mniej niż 1000, podzielonych na kategorie.
3. W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
4. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.

Wymagane funkcje VPN systemu:

1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
5. Obsługa Dead Peer Detection (DPD).
6. Wsparcie dla IKEv1 i IKEv2.
7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.

10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.
12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.

Zarządzanie:

1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.
8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.

Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania:

1. Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
2. Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
3. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
4. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline
5. Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
6. Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
7. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
8. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
9. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
10. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
11. Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
12. Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
13. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
14. Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
15. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
16. System ma mieć możliwość generowania raportów w formacie PDF oraz opcję eksportowania szczegółowych informacji do pliku CSV.
17. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
18. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
19. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
20. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.

21. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
22. Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów