załącznik nr 3 - Opis przedmiotu zamówienia

dla postępowania o udzielenie zamówienia na

dostawę, instalację i konfigurację sprzętu IT oraz licencje, w miejscach docelowych wskazanych przez Mazowiecki Szpital Onkologiczny w Wieliszewie, w ramach projektu *Budowa internetowej platformy elektronicznych usług publicznych e-szpital oraz wdrożenie elektronicznej dokumentacji medycznej w Mazowieckim Szpitalu Onkologicznym w Wieliszewie* w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020, oś priorytetowa II „Wzrost e-potencjału Mazowsza” dla działania 2.1 „E-usługi”, poddziałanie 2.1.1 *E-usługi dla Mazowsza* ***–*** typ projektu e-zdrowie.

W skład zamówienia wchodzą następujące elementy:

**1. Serwer aplikacji (1 szt.)**

**Obudowa**

Maksymalnie 2U RACK 19 cali (wraz z szynami umożliwiającymi wysunięcie oraz ramieniem do prowadzenia kabli i wszystkimi elementami niezbędnymi do zamontowania serwera w szafie).

**Procesor**

Minimum dwa procesory minimum dwunastordzeniowe, o częstotliwości co najmniej 2.2GHz, minimum 30MB cache, osiągające w oferowanym serwerze w testach SPECint\_rate2006 wynik nie gorszy niż 1770 punktów oraz w testach SPECint\_rate\_base2006 wynik nie gorszy niż 1710 punktów. Wynik testu dla oferowanego serwera musi być opublikowany na stronie  [www.spec.or](http://www.spec.org/)g

**Liczba procesorów**

Minimum 2

**Pamięć operacyjna**

Minimum 512 GB RDIMM DDR4 Dual Rank (pojedyncze kości minimum 32GB) minimum 2400MHz z możliwością rozbudowy do minimum 3TB. Minimum 24 sloty na pamięć.

**Sloty rozszerzeń**

Minimum 6 slotów PCI-Express Generacji 3 Full-height, w tym minimum 4 sloty x16 i minimum dwa sloty Full-length.

**Dysk twardy**

Minimum 8 miejsc na dyski typu Hot Swap, SAS/SATA/SSD 2,5” z możliwością rozbudowy do

24. Zainstalowane minimum 4 dyski SAS 12G 300GB 15K.

**Inne**

Wbudowany wewnętrzny napęd DVD-RW.

**Kontroler**

Kontroler macierzowy nie zajmujący wymaganych slotów PCI, SAS 12Gb z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Możliwość rozbudowy pamięci cache do 4GB poprzez rozbudowę lub wymianę kontrolera.

**Interfejsy sieciowe**

Minimum 4 wbudowane porty Ethernet 10/100/1000 Mb/s RJ45 z możliwością rozbudowy do minimum 8bez zajmowania wymaganych slotów PCI-Express.

**Interfejsy FC**

Minimum 2 karty FC 8Gb SW LC

**Karta graficzna**

Zintegrowana karta graficzna

**Porty**

4 porty RJ-45 1 port RJ-45 dedykowany dla interfejsu zdalnego zarządzania 7 x USB (w tym minimum 3 z przodu i dwa z tyłu obudowy)

2 x VGA, 1 z przodu i 1 z tyłu obudowy Wewnętrzny slot na kartę SD

1 port szeregowy nie zajmujący wymaganych slotów PC

**Zasilacz**

Minimum 2 szt. min 800W, typ Hot-plug, redundantne o sprawności minimum 94%

**Chłodzenie**

Zestaw wentylatorów redundantnych typu hot-plug Możliwość pracy serwera w temperaturze otoczenia do 45st.C

**Zarządzanie i obsługa techniczna**

Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) z dedykowanym portem RJ45 pozwalającą na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Karta musi zapewniać możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD/DVD/ISO i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe i nie zajmująca wymaganych slotów PCI. Jeśli jest wymagana to załączona odpowiednia licencja.

**Wsparcie dla Systemów Operacyjnych i Wirtualizacyjnych**

Microsoft Windows Server min. w wersji 2012R2, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), VMware, Citrix XenServer

**Gwarancja**

Minimum 5 lat, realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy do 6 godzin w miejscu instalacji, z pozostawieniem uszkodzonych dysków u zamawiającego realizowany przez polski oddział serwisu producenta.

**Inne**

Zainstalowany z przodu obudowy panel udostępniający informacje o takich elementach jak: procesory, pamięci, wentylatory, karty sieciowe, zasilacze, sloty PCI, temperatura, numer SN.

**2. Serwery bazodanowe (2 szt.)**

**Obudowa**

Maksymalnie 2U RACK 19 cali (wraz z szynami umożliwiającymi wysunięcie oraz ramieniem do prowadzenia kabli i wszystkimi elementami niezbędnymi do zamontowania serwera w szafie)

**Procesor**

Minimum jeden procesor, minimum osiemnastordzeniowy, o częstotliwości co najmniej 2.3GHz, minimum 45MB cache, osiągające w oferowanym serwerze wyniki w testach dla konfiguracji dwuprocesorowych SPECint\_rate2006 wynik nie gorszy niż 1550 punktów oraz w testach SPECint\_rate\_base2006 wynik nie gorszy niż 1490 punktów. Wynik testu dla oferowanego serwera musi być opublikowany na stronie  [www.spec.or](http://www.spec.org/)g

**Liczba procesorów**

Minimum 1

**Pamięć operacyjna**

Minimum 192 GB RDIMM DDR4 Dual Rank (pojedyncze kości minimum 16GB) minimum 2400MHz z możliwością rozbudowy do minimum 3TB. Minimum 24 sloty na pamięć.

**Sloty rozszerzeń**

Minimum 6 slotów PCI-Express Generacji 3 Full-height, w tym minimum 4 sloty x16 i minimum dwa sloty Full-length.

**Dysk twardy**

Minimum 8 miejsc na dyski typu Hot Swap, SAS/SATA/SSD 2,5” z możliwością rozbudowy do 24. Zainstalowane minimum 4 dyski SAS 12G 300GB 15K.

**Inne**

Wbudowany wewnętrzny napęd DVD-RW.

**Kontroler**

Kontroler macierzowy nie zajmujący wymaganych slotów PCI, SAS 12Gb z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Możliwość rozbudowy pamięci cache do 4GB poprzez rozbudowę lub wymianę kontrolera.

**Interfejsy sieciowe**

Minimum 4 wbudowane porty Ethernet 10/100/1000 Mb/s RJ45 z możliwością rozbudowy do minimum 8bez zajmowania wymaganych slotów PCI-Express.

**Interfejsy FC**

Minimum 2 karty FC 8Gb SW LC

**Karta graficzna**

Zintegrowana karta graficzna

**Porty**

4 porty RJ-45

1 port RJ-45 dedykowany dla interfejsu zdalnego zarządzania

7 x USB (w tym minimum 3 z przodu i dwa z tyłu obudowy) 2 x VGA, 1 z przodu i 1 z tyłu obudowy

Wewnętrzny slot na kartę SD

1 port szeregowy nie zajmujący wymaganych slotów PCI

**Zasilacz**

Minimum 2 szt. min 800W, typ Hot-plug, redundantne o sprawności minimum 94%

**Chłodzenie**

Zestaw wentylatorów redundantnych typu hot-plug Możliwość pracy serwera w temperaturze otoczenia do 45st.C

**Zarządzanie i obsługa techniczna**

Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) z dedykowanym portem RJ45 pozwalającą na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Karta musi zapewniać możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD/DVD/ISO i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe i nie zajmująca wymaganych slotów PCI. Jeśli jest wymagana to załączona odpowiednia licencja.

Wsparcie dla Systemów Operacyjnych i Wirtualizacyjnych Microsoft Windows Server min. w wersji 2012R2, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), VMware, Citrix, XenServer

**Gwarancja**

Minimum 5 lat, realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy do 6 godzin w miejscu instalacji~~,~~ z pozostawieniem uszkodzonych dysków u zamawiającego realizowany przez polski oddział serwisu producenta.

**Inne**

Zainstalowany z przodu obudowy panel udostępniający informacje o takich elementach jak: procesory, pamięci, wentylatory, karty sieciowe, zasilacze, sloty PCI, temperatura, numer SN.

**3. Macierze dyskowe (2 szt.)**

Minimalne technicznych parametry dla pojedynczej macierzy dyskowej:

1. Zewnętrzna macierz dyskowa wyposażona w dwa kontrolery macierzowe pracujące w trybie active – active wyposażone w minimum 6GB Cache per kontroler.
2. Po zaniku zasilania zawartość pamięci Cache powinna być podtrzymywana bateryjnie przez min. 96h lub z zastosowaniem innej technologii przynajmniej 1 rok.
3. Macierz przystosowana do montażu w szafie rack 19”
4. Macierz musi posiadać następujące komponenty wymieniane w trybie “hot plug” : HDD, kontrolery macierzowe, wentylatory i zasilacze.
5. Oferowana macierz musi wspierać poziomy Raid 0, Raid 1, Raid 1+0, Raid 3, Raid 5, Raid

5+0, Raid 6.

1. Oferowana macierz musi pozwalać skonfigurować minimum 512 LUN o rozmiarze LUN nie mniej niż 128TB z poziomu macierzy dyskowej.
2. Macierz powinna wspierać przynajmniej następujące typy dysków twardych: SSD, SAS i

NL-SAS

1. Macierz musi wspierać dyski: min. 400GB SSD, 300/450/600/900/1200GB SAS oraz 1TB, 2TB, 3TB, 4TB, 6TB, 8TB NL-SAS. Macierz musi się rozbudować do min. 190 dysków w ramach oferowanych kontrolerów macierzowych.
2. Macierz musi być wyposażona w 4 dyski SAS SSD o pojemności min 200GB oraz 30 dysków SAS 10000rpm o pojemności min 1,2TB. Macierz musi posiadać min. 54800 GB przestrzeni dyskowej RAW.
3. Oferowana macierz musi posiadać minimum 2 porty FC 8Gb front-end i minimum 2 porty 1Gb iSCSI per kontroler umożliwiające dołączenie macierzy bezpośrednio do serwerów lub przełączników. Oferowana macierz musi posiadać min. 1 port SAS 6Gb/s per kontroler do podłączenia dodatkowych półek dyskowych.
4. Oferowana macierz musi posiadać pełną redundancję zasilania i wentylacji
5. Oferowana macierz musi zapewniać możliwość wykonywania szybkich kopi danych typu Snapshot i Clone dysków logicznych na poziomie kontrolerów macierzowych. Oferowana macierz musi wspierać min. 256 snapshoty w ramach macierzy dyskowej.
6. Oferowana macierz musi umożliwiać tworzenie wolumenów w trybie Thin Provisioning. Jeżeli taka funkcjonalność jest licencjonowana należy załączyć licencję na maksymalną wspieraną pojemność dyskową urządzenia
7. Oferowana macierz musi umożliwiać rozszerzenie pamięci Cache kontrolera do odczytu o przestrzeń na dyskach SSD.
8. Oferowana macierz musi umożliwiać skorzystanie z tzw. Sub-LUN Tiering czyli możliwości migracji bloków danych dysku logicznego na podstawie analizy ich aktywności przez macierz (najbardziej i najmniej aktywne) pomiędzy trzema typami dysków (SSD, SAS, NL SAS).
9. Oferowana macierz musi pozwalać na replikację danych przynajmniej asynchroniczną z drugą macierzą. Funkcjonalność replikacji musi być realizowana na poziomie kontrolerów macierzowych bez obciążania tym procesem serwerów.
10. Wsparcie dla systemów Windows, Linux, Vmware.
11. Gwarancja - minimum 5 lat, realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy do 6 godzin w miejscu instalacji, z pozostawieniem uszkodzonych dysków u zamawiającego realizowany przez polski oddział serwisu producenta.
12. Oferowana macierz musi posiadać certyfikat Energy Star lub równoważny.
13. Macierz powinna zapewniać skalowalność i rozbudowę w okresie późniejszym.

**4. Urządzenie do archiwizacji NAS (1 szt.)**

**Informacje ogólne**

Pamięć masowa z fabrycznie zainstalowanym oprogramowaniem minimum Windows Storage Server 2012 R2 Standard Edition lub oprogramowanie równoważne (w pełni kompatybilne ze sprzętem i oprogramowaniem działającym u Zamawiającego np.: Windows 2008, 2012, itp. Z możliwością podłączenia do usługi Active Directory ). Synchronizacja i udostępnianie plików, deduplikacja, migawki, replikacja, klasyfikacja plików, limity, monitorowanie plików, raporty dotyczące pamięci masowej

**Obudowa**

Obudowa gotowa do montażu w serwerowej szafie przemysłowej 19” typu RACK maksymalnie 2U wraz z szynami umożliwiającymi wysunięcie i ramieniem do prowadzenia kabli.

**Procesor**

Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Zainstalowany minimum jeden procesor minimum sześciordzeniowy, pamięć cache L3 min 15MB; taktowanie minimum 1,9GHz

**Pamięć operacyjna**

Minimum 16GB (minimum 2 moduły 8GB) RDIMM DDR4 2133MHz, z możliwością rozbudowy. Minimum 24 sloty na pamięć.

**Kontrolery RAID**

Macierzowy SAS 12 Gb/s z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania typu flash, obsługujący poziomy: RAID

0/1/1+0/5/50/6/60.

**Dyski**

Zainstalowane dyski typu HotPlug:

minimum dwa dyski minimum 120GB 6G SFF SSD oraz minimum osiem dysków minimum 2TB SAS 6G LFF o pojemności łącznej minimum 16TB i miejscem na dodatkowe minimum cztery dyski LFF.

**Karty sieciowe**

Minimum 4 wbudowane porty Ethernet 10/100/1000 Mb/s RJ45 z możliwością rozbudowy do minimum 8 bez zajmowania wymaganych slotów PCI-Express.

**Porty**

4 x USB 2.0

5 x RJ-45 w tym jeden dedykowany do zarządzania

VGA

**Sloty rozszerzeń**

Minimum 3 sloty PCIe 3.0 pełnej wysokości, w tym minimum dwa gniazda x16.

**Inne**

Urządzenie oraz jego komponenty składowe muszą być fabrycznie nowe.

Urządzenie oraz jego komponenty składowe muszą być wyprodukowane nie wcześniej niż 6 miesięcy przed terminem dostawy.

Urządzenie oraz jego komponenty składowe muszą pochodzić z autoryzowanego kanału sprzedażowego producenta.

Urządzenia muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.

Urządzenie oraz jego komponenty składowe muszą być dostarczone w oryginalnych opakowaniach fabrycznych.

Zintegrowane z płytą główną złącze na moduł TPM

Urządzenie musi być wyposażony w kartę zdalnego zarządzania (konsoli) z dedykowanym portem RJ45 pozwalającą na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Karta musi zapewniać możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD/DVD/ISO i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe i nie zajmująca wymaganych slotów PCI. Jeśli jest wymagana to załączona odpowiednia licencja.

Zasilanie i chłodzenie

Zasilacze 2 sztuki min 800W, typ Hot-plug, redundantne, o sprawności minimum 94% Zestaw redundantnych wentylatorów typu hot-plug

**Gwarancja**

Minimum 5 lat, realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy do 6 godzin w miejscu instalacji z pozostawieniem uszkodzonych dysków u zamawiającego realizowany przez polski oddział serwisu producenta.

**5. Przełącznik sieciowy (2 szt.)**

**Interfejsy**

Min. 24 porty 8Gb FC z czego aktywne minimum 8 portów z możliwością rozszerzenia do min 24.

**Obudowa**

Przystosowana do montażu w szafie rack 19”, wysokość 1U

**Dodatkowe funkcje**

Możliwość aktualizacji oprogramowania bez zakłócania pracy, możliwość aktywacji licencji na dodatkowe porty bez zakłócania pracy.

**Zarządzanie**

Web Tools

Enhanced Group Management (EGM) Radius

API

IP SNMP

**Inne**

Dołączone kable Multi-mode LC-LC o długości 5 m, min. 8 szt. oraz odpowiednie interfejsy optyczne SFP+ min. 8 szt.

**Gwarancja**

Minimum 5 lat, realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy do 6 godzin w miejscu instalacji, z pozostawieniem uszkodzonych dysków u zamawiającego realizowany przez polski oddział serwisu producenta.

Przełączniki sieciowe mają być połączone w sieci już z istniejącymi, które powinny zostać rozbudowane o gniazda światłowodowe Transceiver ProCurve J8706A w ilości 6 szt., w celu kompatybilności całości budowanej platformy IT.

**6. Kontrolery Access Point (2 szt.)**

Funkcja zapory sieciowej

1. Kontroler musi spełniać co najmniej funkcje: a. Kontrolera sieci bezprzewodowej dla wskazanej ilości punktów dostępowych b. Pełnostanowej zapory sieciowej (stateful firewall)

1. VPN Gateway
	1. Kontroler musi umożliwiać współpracę z zewnętrznym systemem uwierzytelniania i

kontroli dostępu klientów. Musi istnieć możliwość rozbudowy kontrolera o nie mniej niż poniższe funkcje:

* Szyfrowanie z wykorzystaniem “Suite-B Cryptography” – AES128-GCM/AES256-GCM
	+ Zdalny dostęp VPN za pomocą klienta Widnows/MAC/iOS/Android

3. Rozbudowa systemu opisana w punkcie 2 musi być realizowana wyłącznie poprzez aktywację licencji, bez konieczności zakupu dodatkowych modułów sprzętowych lub dodatkowych urządzeń.

4. Kontroler musi zapewniać możliwość integracji w przyszłości z innymi kontrolerami różnej

wielkości, pracując w systemie hierarchicznym.

1. Komunikacja pomiędzy kontrolerami musi wykorzystywać protokoły sieciowe niewymagające instalacji dodatkowych urządzeń sieciowych.
2. Kontroler musi zapewniać centralne zarządzanie wszystkimi punktami dostępowymi w sieci, łącznie z tworzeniem i zarządzaniem obrazami konfiguracyjnymi oraz aktualizacją oprogramowania.
3. Kontroler musi posiadać następujące parametry sieciowe:

a. możliwość wdrożenia w warstwie 2 i 3 ISO/OSI,

b. Wsparcie dla sieci VLAN w tym również trunk 802.1q c. Wbudowany serwer DHCP

d. Obsługa SNMPv2, SNMPv3 e. Ruting dynamiczny OSPF

* 1. Kontroler sieci WLAN musi obsługiwać nie mniej niż:

a. Metody szyfrowania i kontroli połączeń: WEP, dynamic WEP, TKIP WPA, WPA2,

AES - CCMP, EAP, PEAP, TLS, TTLS, LEAP, EAP-FAST , DES, 3DES, AES-CBC

b. Obsługa szyfrowania AES-CCM, TKIP i WEP centralnie na kontrolerze c. Obsługa SSL i TLS, RC4 128-bit oraz RSA 1024 i 2048 bit

d. Autoryzacja dostępu użytkowników:

* Typy uwierzytelnienia: IEEE 802.1X (EAP,LEAP,PEAP,EAP-TLS,EAP-TTLS, EAP-FAST), RFC 2548, RFC 2716 PPP EAP-TLS, RFC 2865 Radius Authentication, RFC 3576 dynamic Auth Ext for Radius, RFC 3579 Radius suport for EAP, RFC 3580, 3748, captive portal”, 802.1X i MAC
* Możliwość wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia
* Wsparcie dla autoryzacji: Microsoft NAP, CISCO NAC, Juniper NAC, Aruba NAC
* Możliwość utworzenia nie mniej niż 16 SSID na jednym punkcie dostępowym. Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania, oddzielnych vlan-ów i oddzielnego portalu „captive portal”
* Możliwość wykorzystania mieszanego szyfrowania dla określonych SSID (np. WPA/TKIP i

WPA2/AES)

* Terminowanie sesji użytkowników sieci bezprzewodowej musi odbywać się na kontrolerze, nie na punkcie dostępowym
* Uwierzytelnienie oraz autoryzacja musi być możliwa przy wykorzystaniu lokalnej bazy danych na kontrolerze oraz zewnętrznych serwerów uwierzytelniających. Kontroler musi wspierać co najmniej następujące serwery AAA: Radius, LDAP, SSL Secure LDAP, TACACs+, Steel Belted Radius Server, Microsoft Active Directory, IAS Radius Server, Cisco ACS Server, RSA ACE Server, Interlink Radius Server, Infoblox, Free Radius.
1. Kontroler musi gwarantować automatyczne przełączenie z zewnętrznego serwera AAA na lokalną bazę danych w przypadku awarii serwerów uwierzytelniających.

f. Musi istnieć mechanizm definiowania ról użytkowników oraz bazując na nich egzekwowania polityki dostępu g. Kontroler musi zapewniać obsługę XML API do uwierzytelnienia

9. Kontroler musi posiadać obsługę transmisji różnego typu danych w jednej sieci: a. Integracja jednoczesnej transmisji danych i głosu

b. Obsługa QoS Voice Flow Classification, SIP, Spectralink SVP, Cisco SCCP, Vocera ALGs, kolejkowanie w powietrzu, obsługa 802.11e-WMM, U-APSD, T-SPEC, SIP authentication tracking, Diff-serv marking, 802.1p

c. Obsługa fast roaming

d. Ograniczanie pasma dla użytkownika oraz dla roli użytkownika

1. Kontroler musi posiadać funkcję adaptacyjnego zarządzania pasmem radiowym:
	* 1. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe
		2. Stałe monitorowanie pasma oraz usług
		3. Rozkład ruchu pomiędzy różnymi punkami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma
		4. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału
		5. Wsparcie dla 802.11h
		6. Integracja z systemami RTLS - wymagane jest wbudowane stosowne API
2. Kontroler musi posiadać funkcję wbudowanej zapory sieciowej, posiadającej nie mniej niż następujące własności:
	1. Inspekcja pakietów z uwzględnieniem reguł bazujących na: użytkownikach, rolach, protokołach i portach, adresacji IP, lokalizacji, czasie dnia
	2. Mirroring sesji
	3. Szczegółowe logi (per packet) do późniejszej analizy
	4. ALG (Application Layer gateway) dla protokołów FTP, TFTP, SIP, SCCP, RTSP, Vocera,

PPTP

* 1. Translacja źródłowa, docelowa adresów IP
	2. Identyfikacja i blokowanie ataków DoS

g. Obsługa protokołu GREmusi być włączana programowo przez dodanie odpowiedniej licencji.

12. Kontroler musi posiadać funkcję systemu WIDS/ WIPS. Moduł WIPS musi posiadać co najmniej następujące funkcje:

* Detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP). Automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów.
* Identyfikacja i możliwość blokowania sieci Adhoc
* Identyfikacja anomalii sieciowych, jak wireless bridge czy Windows client bridging
* Ochrona przed atakami sieciowymi na sieć bezprzewodową
* Identyfikacja podszywania się pod autoryzowane punkty dostępowe
	1. Kontroler musi posiadać funkcję analizatora widma. Włączenie analizatora widma musi być możliwe w dwuradiowych punktach dostępowych w trybie pracy wyłącznie jako analizator oraz w trybie hybrydowym, gdzie punkt zarówno analizuje widmo jak i obsługuje ruch użytkowników. Funkcje WIPS/WIDS oraz analizy widma muszą być włączane programowo przez dodanie odpowiednich licencji.

14. Kontroler musi mieć wbudowany serwer VPN, charakteryzujący się następującymi parametrami, nie mniej niż:

a. Site-to-site oraz client-site VPN

b. Terminacja ruchu L2TP/IPSEC VPN, XAUTH/IPSEC, PPTP

* 1. Obsługa tokenów
	2. Wsparcie dla serwerów Radius i LDAP w celu uwierzytelnienia sesji VPN przy użyciu:

PAP CHAP, MS-CHAP, MS-CHAP2

* 1. Wsparcie dla algorytmów kryptograficznych: DES, 3DES, AES przy wykorzystaniu dedykowanych układów scalonych kontrolera
1. Zarządzanie kontrolerem musi odbywać się poprzez co najmniej następujące metody:

interfejs przeglądarki Web (https), linia komend przez SSH i dedykowany port konsoli System sieci bezprzewodowej musi umożliwiać jej rozbudowę o dodatkowe kontrolery. W celu zapewnienia centralnego zarządzania większą ilością kontrolerów producent musi posiadać w swojej ofercie rozwiązanie, umożliwiające spójne zarządzanie siecią WLAN, również heterogeniczną złożoną z produktów wielu producentów

16. Wymagane parametry zamawianego kontrolera:

a. Ilość możliwych obsługiwanych punktów dostępowych nie mniej niż 64 b. Ilość jednocześnie obsługiwanych użytkowników nie mniej niż 4k

1. Ilość aktywnych sesji zapory sieciowej nie mniej niż 64k, przepustowość zapory sieciowej nie mniej niż 8Gbps

d. Ilość jednoczesnych tuneli IPSEC nie mniej niż 2k

e. Przepustowość ruchu szyfrowanego nie mniejsza niż 2 Gbps dla algorytmu 3DES, 4Gbps dla algorytmu AES - CCM

f. 8 interfejsów Gigabit Ethernet wyposażonych w styk miedziany g. 1 interfejs konsoli (RS-232) RJ-45

h. Zasilanie AC 100-240V, 50-60Hz

17. Kontroler musi zostać dostarczony z licencjami do obsługi minimum 50 punktów dostępowych, zapory sieciowej oraz WIDS/WIPS i analizatora widma.

Wymagana zgodność z normami: a. EN 55022 Class B

* 1. IEC/EN 60950
	2. CE Marking
1. Kontroler musi być objęty wsparciem technicznym polskiego centrum

serwisowego na okres minimum 60 miesięcy, realizowanym w trybie wysyłki urządzenia w ciągu maksymalnie 10 dni roboczych po zgłoszeniu problemu.

Zamawiający musi mieć dostęp do aktualizacji oprogramowania przez okres minimum 36 miesięcy od momentu dostarczenia kontrolera.

**7. Access Point (50 szt.)**

1.Punkt dostępowy do montażu wewnątrz budynków, pracujący w dwóch kanałach radiowych jednocześnie (obsługując standardy 802.11an, 802.11bgn, 802.11ac).

2. Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej.

1. W system operacyjny musi być wbudowana pełno stanowa zapora sieciowa z funkcją rozpoznawania aplikacji.
2. W system musi być wbudowany serwer DHCP.
3. W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów.
4. Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach: a. EAP-TLS

b. PEAP-MSCHAPv2

c. PEAP-GTC

d. TTLS-MSCHAPv2

1. Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS

oraz LDAP.

8.Punkt dostępowy musi obsługiwać nie mniej niż 5 niezależnych SSID. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN.

* 1. Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej:
1. Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania
2. Zewnętrzny portal WWW
	1. Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT.
	2. Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne oraz umożliwiać ich tworzenie przez użytkowników bez uprawnień administracyjnych
	3. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:

a. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe

b. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu c. Rozkład ruchu pomiędzy różnymi punkami dostępowym bazując na ilości użytkowników oraz utylizacji pasma

d. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału

e. Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie

802.11n oraz starszych (802.11a/b/g) f. Wsparcie dla 802.11d oraz 802.11h

1. Obsługa tzw. „Sticky Clients” polegająca na automatycznym przełączaniu klientów do punktu dostępowego oferującego najlepszy sygnał
2. Możliwość przełączenia AP w tryb analizatora widma w celu analizy zakłóceń pochodzących od innych źródeł interferencji niż sieci WiFi
	1. Obsługa roamingu klientów w warstwie 2
	2. Obsługa roaminu klientów w warstwie 3 pomiędzy różnymi grupami punktów dostępowych, z zachowaniem adresu IP klienta
	3. Obsługa szybkiego roamingu klientów pomiędzy punktami dostępowymi z wykorzystaniem nie mniej niż:
3. Opportunistic Key Caching
4. 802.11r

c. 802.11v

1. 802.11k
	1. Obsługa monitoringu przez SNMP v1/2/3
	2. Obsługa logowania na zewnętrznym serwerze SYSLOG
	3. W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci
	4. W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci
	5. Musi istnieć możliwość centralnego zarządzania systemem punktów bezprzewodowych za pomocą zewnętrznego oprogramowania, które nie jest przedmiotem postępowania
	6. Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:
* Widok diagnostyczny prezentujący problemy z sygnałem/prędkością
* Wykorzystanie pasma
* Ilość klientów korzystających z systemu/interferujących
* Ilość ramek wejściowych/wyjściowych dla każdego radia
* Ilość odrzuconych/błędnych ramek/s dla każdego radia
* Szum tła dla każdego radia
* Wyświetlanie logów systemowych
	1. Punkt dostępowy musi posiadać cztery wewnętrzne anteny 2x2 MIMO, o

wzmocnieniu co najmniej: 4 dBi dla 2.4GHz oraz 6 dBi dla 5GHz

1. Punkt dostępowy musi obsługiwać klientów 2x2:2 w trybie SU-MIMO
2. Punkt dostępowy musi oferować następujące mechanizmy poprawiające efektywność działania sieci radiowej, nie mniej niż:

a. MRC – Maximum Radio Combining b. ACC – Advanced Cellular Coexistence c. STBC – Space-Time Block Coding

d. LDPC – Low-density Parity Check e. TxBF – Transmit Beamforming

25. Specyfikacja radia 802.11a/n/ac:

a. Moc wyjściowa nie mniej niż 21dBm (18dBm per łańcuch nadawczy) b. Obsługiwane częstotliwości:

* 5.150 ~ 5.250 GHz (low band)
* 5.250 ~ 5.350 GHz (mid band)
* 5.470 ~ 5.725 GHz (Europa)
* 5.725 ~ 5.825/5.850 GHz (pasmo licencjonowane)

c. Technologie obsługiwane: orthogonal frequency division multiplexing (OFDM) d. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM

e. Moc transmisji konfigurowalna przez administratora – możliwość dwukrotnego zwiększenia/zmniejszenia mocy (o +/-3dB)

1. Prędkości transmisji: 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a/g, 802.11n MCS0-MCS23 (6,5Mbps do 450Mbps), 802.11ac MCS0 do MCS9, NSS = 1 do 2 (6.5 do 867 Mbps)
2. Obsługa HT – kanały 20, 40 oraz VHT 20/40/80MHz
	1. Specyfikacja radia 802.11b/g/n:

a. Moc wyjściowa nie mniej niż 21dBm (18dBm per łańcuch nadawczy) b. Częstotliwość 2,400 ~2,4835GHz

c. Technologia direct sequence spread spectrum (DSSS) oraz OFDM d. Typy modulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM

e. Moc transmisji konfigurowalna przez administratora – możliwość dwukrotnego zwiększenia/zmniejszenia mocy (o +/-3dB)

f. Prędkości transmisji: 6,9,12,18,24,36,48,54 Mbps dla 802.11g

g. Prędkości od MCS0 do MCS15 (6.5 Mbps do 300 Mbps) dla 802.11n

1. Obsługa HT – kanały 20 oraz 40MHz
	1. Punkt dostępowy musi posiadać co najmniej:

a. 1 interfejs 10/100/1000 Base-T WAN z możliwością zasilania przez zasilacz PoE 802.3af oraz 802.3at

b. 1 interfejs konsoli RS-232 RJ45 c. zasilanie 12V DC

d. przycisk przywracający konfigurację fabryczną e. Zaczep linki zabezpieczającej (Kensington)

1. Urządzenie musi być dostarczone elementem do montażu na suficie podwieszanym
2. Parametry pracy urządzenia:

a. Temperatura otoczenia: 0-40 º C

1. Wilgotność 5% - 95%

c. Obsługiwane standardy:

* Ethernet IEEE 802.3 / IEEE 802.3u
* 802.3az Energy Efficient Ethernet (EEE)
* Wireless IEEE 802.11a/b/g/n/ac

d. Znak CE e. EN 300 328 f. EN 301 489

1. EN 60950
	1. Ograniczona dożywotnia gwarancja – punkty dostępowe muszą być objęte gwarancją

przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 45 dni przesyła zamiennik. Gwarancja nie wymaga zakupu/posiadania ważnego kontraktu wsparcia technicznego.

30. Wsparcie techniczne, aktualizacje oprogramowania oraz gwarancja na okres minimum 60 miesięcy realizowane przez polskojęzyczne centrum pomocy technicznej. Zgłaszanie incydentów przez portal WWW, pocztę i telefon 24/7/365. Wymiana uszkodzonego urządzenia w przeciągu maksymalnie 10 dni roboczych od zgłoszenia awarii.

**8. Urządzenie UTM wraz z systemem antywirusowym (1 szt.)**

**OBSŁUGA SIECI**

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.

**ZAPORA KORPORACYJNA (Firewall)**

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (część jako router, a część jako bridge).
4. Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba

administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.

1. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall’u.
2. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).
3. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).

**INTRUSION PREVENTION SYSTEM (IPS)**

1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
2. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej.
5. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
6. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola

DSCP.

**KSZTAŁTOWANIE PASMA (Traffic Shapping)**

1. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
2. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
3. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

**OCHRONA ANTYWIRUSOWA**

1. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
4. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W

przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.

**OCHRONA ANTYSPAM**

1. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
2. Ochrona antyspam ma działać w oparciu o:
	1. białe/czarne listy,
	2. DNS RBL,
	3. heurystyczny skaner.
3. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.
4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

**WIRTUALNE SIECI PRYWANTE (VPN)**

1. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń

VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).

1. Odpowiednio kanały VPN można budować w oparciu o:
	1. PPTP VPN,
	2. IPSec VPN,
	3. SSL VPN
2. SSL VPN musi działać w trybach Tunel i Portal.
3. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
4. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
5. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.

**FILTR DOSTĘPU DO STRON WWW**

1. Urządzenie ma posiadać wbudowany filtr URL.
2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
3. Administrator musi mieć możliwość dodawania własnych kategorii URL.
4. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.
5. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.
6. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:
	1. blokowanie dostępu do adresu URL,
	2. zezwolenie na dostęp do adresu URL,
	3. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
7. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
8. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.
9. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.
10. Urządzenie posiada możliwość identyfikacji oraz blokowanie przesyłanych danych z wykorzystaniem typu MIME.
11. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.
12. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http.

**UWIERZYTELNIANIE**

1. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:
	1. lokalną bazę użytkowników (wewnętrzny LDAP),
	2. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
	3. usługę katalogową Microsoft Active Directory.
2. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:
	1. SSL,
	2. Radius,
	3. Kerberos.
3. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Active Directory.
4. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.
5. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.

**ADMINISTRACJA ŁĄCZAMI OD DOSTAWCÓW USŁUG INTERNETOWYCH (ISP).**

1. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
	1. równoważenie względem adresu źródłowego,
	2. równoważenie względem adresu źródłowego i docelowego (połączenia).
3. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do internetu.
4. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
5. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów.
6. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
7. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
8. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIP, OSPF oraz BGP.
9. Rozwiązanie powinno wspierać technologię Link Aggregation.

**POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA**

1. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.
2. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP

– DHCP Relay.

1. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.
2. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS
3. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.
4. Urządzenie musi posiadać usługę DNS Proxy.

**ADMINISTRACJA URZĄDZENIEM**

1. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.
2. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
3. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
4. Komunikacja może odbywać się na porcie innym niż https (443 TCP).
5. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
6. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog).
7. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.
8. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.

**RAPORTOWANIE**

1. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.
4. System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów.
5. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu.
6. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
7. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy

**PARAMETRY SPRZĘTOWE**

1. Urządzenie ma być wyposażone w dysk twardy o pojemności co najmniej 320 GB.
2. Liczba portów Ethernet 10/100/1000 – min. 8.
3. Możliwość rozszerzenia ilości interfejsów Ethernet 10/100/1000 do min. 16.
4. Możliwość zastosowania nie mniej niż 4 interfejsów światłowodowych o przepustowości

1Gb.

1. Możliwość wykorzystania nie mniej niż 2 interfejsów światłowodowych o przepustowości

10Gb.

1. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G.
2. Przepustowość Firewalla – min. 10 Gbps
3. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 7 Gbps.
4. Przepustowość filtrowania Antywirusowego – min. 1,6 Gbps
5. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 2,4 Gbps.
6. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 1 000.
7. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 150
8. Obsługa min. 280VLAN
9. Liczba równoczesnych sesji - min. 1 000 000 i nie mniej niż 40 000 nowych sesji/sekundę.
10. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
11. Urządzenie jest nielimitowane na użytkowników.

**ASYSTA TECHNICZNA I SERWIS**

Producent zapewni wsparcie techniczne, aktualizacje oprogramowania oraz gwarancja na okres minimum 60 miesięcy realizowane przez polskojęzyczne centrum pomocy technicznej. Zgłaszanie incydentów przez portal WWW, pocztę i telefon. Wymiana uszkodzonego urządzenia w przeciągu maksymalnie 10 dni roboczych od zgłoszenia awarii. Producent lub autoryzowany serwis wdroży administratora do zarządzania i konfiguracji urządzenia.

**OPROGRAMOWANIE ANTYWIRUSOWE**

W celu zapewnienia bezpieczeństwa budowanej platformy w ramach urządzenia UTM będzie zainstalowany system antywirusowy (zgodnie z pkt. 20 specyfikacji niniejszego urządzenia) z licencja na 150 stacji roboczych i 9 serwerów o następujących parametrach:

1. Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.
4. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim.
5. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
11. Możliwość skanowania dysków sieciowych i dysków przenośnych.
12. Skanowanie plików spakowanych i skompresowanych.
13. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).
14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
15. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
16. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
17. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
18. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
19. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
20. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
21. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
22. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i

Windows Live Mail.

1. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
2. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
3. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
4. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
5. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.
6. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
7. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
8. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
9. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
10. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
11. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
12. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
13. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
14. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
15. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.
16. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
17. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
18. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
19. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
20. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
21. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
22. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
23. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
24. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
25. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
26. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
27. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
28. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
29. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
30. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu.
31. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
32. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.
33. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.
34. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
35. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
36. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
37. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
38. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
	* + tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
		+ tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
		+ tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
		+ tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
		+ Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
39. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
40. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
41. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
42. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
43. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
44. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
45. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
46. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
47. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
48. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
49. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
50. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
51. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
52. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
53. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
54. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
55. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.
56. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
57. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
58. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
59. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.
60. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
61. Możliwość podejrzenia licencji za pomocą, której program został aktywowany.

**Ochrona serwera plików Windows**

1. Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012

R2, SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012.

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Wbudowana technologia do ochrony przed rootkitami i exploitami.
4. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
5. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
6. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
8. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
9. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
10. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
11. Możliwość skanowania dysków sieciowych i dysków przenośnych.
12. Skanowanie plików spakowanych i skompresowanych.
13. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (z uwzględnieniem plików bez rozszerzeń).
14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
15. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.
16. Aplikacja powinna wspierać mechanizm klastrowania.
17. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
18. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
19. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
20. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych

FireWire.

1. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia.
2. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika.
3. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.
4. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
5. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
6. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
8. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
9. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
10. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
11. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
12. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
13. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
14. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
15. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
16. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
17. Aktualizacje modułów analizy heurystycznej.
18. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
19. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
20. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania
	1. lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
21. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
22. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
23. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
24. Interfejs programu ma oferować funkcję pracy w trybie bez grafiki gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.
25. Interfejs programu ma mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb wysokiego kontrastu.
26. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
27. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
28. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.
29. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.
30. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
31. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu.
32. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
33. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
34. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
35. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz urządzeń USB.
36. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
37. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
38. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
39. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
40. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
41. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
42. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).
43. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu.
44. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
45. Aplikacja musi wspierać skanowanie magazynu Hyper-V
46. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów
47. Praca programu musi być niezauważalna dla użytkownika.
48. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
49. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

**Administracja zdalna**

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows

Server 2003, 2008, 2012 oraz systemach Linux.

1. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).
2. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych

MS SQL i MySQL.

1. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika.
2. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.
3. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
4. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
5. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
6. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.
7. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
8. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu

SSL.

1. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
2. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
3. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.
4. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.
5. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
6. Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym.
7. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
8. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
9. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.
10. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
11. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
12. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows.
13. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
14. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
15. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
16. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
17. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej
18. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
19. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
20. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.
21. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny.
22. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
23. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
24. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
25. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.
26. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
27. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
28. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
29. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
30. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
31. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
32. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
33. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
34. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.
35. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
36. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
37. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
38. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
39. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
40. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.
41. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
42. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
43. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
44. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
45. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
46. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.
47. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
48. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy

sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.

1. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
2. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.
3. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
4. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.
5. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.
6. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta
7. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
8. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
9. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
10. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp.
11. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania.
12. Serwer administracyjny musi być wyposażona w mechanizm importu oraz eksportu szablonów raportów.
13. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów.
14. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.
15. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
16. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie.
17. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
18. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
19. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
20. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
21. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania.
22. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
23. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
24. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
25. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
26. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
27. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
28. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
29. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i

IPv6 lub wyszukania konkretnej nazwy zagrożenia.

1. Serwer administracyjny musi być wyposażona w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.
2. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).

**9. Stacje robocze typ All In One wraz z klawiaturą
i myszą (30 szt.)**

Procesor

Czterordzeniowy, pamięć podręczna min. L3 8MB.

Dysk twardy

Co najmniej 1 TB

Pamięć RAM

Co najmniej DDR3 16GB

Ekran

21.5-inch IPS Full HD (1920 x 1080) diagonal widescreen WLED backlit anti-glare LCD

Licencje

Windows 10 64 bit z pakietem biurowym Microsoft Office co najmniej 2013 lub równoważny, pozwalający na podłączenie do usługi Active Directory uruchomionej na serwerze z systemem operacyjnym Windows 2008R2. Pakiet biurowy powinien pozwalać na otwarcie, zapis i edycję dokumentów zapisanych w programie Microsoft Office 2013, który Zamawiający posiada, jak również program do obsługi poczty elektronicznej pozwalający na bezproblemową obsługę i podłączenie do istniejącego serwera pocztowego Microsoft Exchange.

 Gwarancja

Co najmniej 60 miesięcy.

**10. Tablety medyczne (12 szt.)**

* System operacyjny x64 dedykowany na urządzenia mobilne, pozwalający na podłączenie urządzenia do istniejącej usługi Active Directory opartej na Windows 2008R2
* Procesor dedykowany do urządzeń mobilnych, co najmniej czterordzeniowy z pamięcią podręczną cache L3 2MB i taktowaniem 1,6 GHz.
* Zintegrowana karta graficzna HD Graphics
* Ekran10.1-inch diagonal full HD (1920 x 1200) wide-viewing angle outdoor display; 16:10 Aspect Ratio z powłoką ochronną Healthcare dedykowany do placówek służby zdrowia.
* Pamięć 4GB LPDDR3 1067 MHz
* Sieć: Wireless connectivity: Broadcom 43241 802.11 a/b/g/n (2x2) + BT 4 LE SDIO
* Porty: I/O: USB 3.0, HDMI in addition to standard power connector
* Zasilanie: 2-cell (30 WHr) polymer Long Life battery

Gwarancja

Co najmniej 60 miesięcy.

**11. Urządzenia wielofunkcyjne (10 szt.)**

Urządzenia monochromatyczne z funkcją duplex z możliwością: drukowania, skanowania, kopiowania. Kompatybilne z systemami Windows 10.

Gwarancja

60 miesięcy

**12. Licencje na serwery**

1. WinSvrStd 2012R2 OLP NL Gov 2Proc 3 szt. lub równoważny pozwalający na podłączenie do istniejącej domeny uruchomionej na serwerze z systemem operacyjnym Windows 2008R2, pozwalający na pracę jako zapasowy kontroler domeny. System powinien posiadać możliwość pracy jako klaster z posiadanym systemem operacyjnym.
2. Licencje dostępowe Windows CAL Device 150 szt. lub równoważne pozwalające na pracę stacji roboczych w usłudze Active Directory uruchomionej u Zamawiającego.