Ośrodek
Badawczo - Rozwojowy
Urządzeń Mechanicznych
"OBRUM" sp. z o.o.

ul. Toszecka 102
44-117 Gliwice
tel: (+48) 32 301 92 09
faks: (+48) 32 231 58 87

www.obrum.gliwice.pl
info@obrum.gliwice.pl

Grupa PGZ
www.pgzsa.pl

Załącznik nr 1 do zapytania ofertowego PLZ/57/2015

OBRUM SP. Z O.O

Konfiguracja infrastruktury na DOSTAWĘ ELEMENTÓW INFRASTRUKTURY PROJEKTU „System inteligentnej analizy wideo do rozpoznawania zachowań i sytuacji w sieciach monitoringu", WYPOSAŻENIE DATA CENTER WRAZ Z MONTAŻEM I URUCHOMIENIEM

Projekt realizowany w ramach przedsięwzięcia pilotażowego Wsparcie badań naukowych i prac rozwojowych w skali demonstracyjnej DEMONSTRATOR+.

8/31/2015

Opracował: M. Michalak

Zaakceptował: T. Czapla

Kierownik Projektu
Tomasz Czapla

INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI

DEMONSTRATOR+

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO

SPIS TREŚCI

1. Cel i zakres

1.1. Słownik pojęć i skrótów

- Projekt „System inteligentnej analizy wideo do rozpoznawania zachowań i sytuacji w sieciach monitoringu" dalej zwany projektem SAVA,
- Zamawiający – OBRUM sp. z o.o.
- CPD – centrum przetwarzania danych,

1.2. Cel dokumentu

Celem dokumentu jest przedstawienie wymagań dla budowy infrastruktury, celem wykorzystania jej w projekcie SAVA. Infrastruktura składa się z trzech części:

- Dostawa urządzeń IT obejmująca swym zakresem dostawę serwerów, macierzy oraz elementów sieciowych,
- Dostawa elementów serwerowni,
- Przystosowanie pomieszczeń serwerowni.

2. Dostawa urządzeń IT

2.1. Ogólny opis zamówienia

Celem Zamówienia jest dostawa infrastruktury na potrzeby pracy Systemów projektu SAVA. *Wyróżniamy następujące elementy infrastruktury:*

- Dostawa infrastruktury sieciowej,
- Dostawa infrastruktury serwerowo-macierzowej,
- Dostawa systemu backupu,

W skład systemów projektu SAVA, obejmujący cały proces przetwarzania gromadzonych danych, wyróżniamy:

- Serwery akwizycji danych,
- Serwery preprocesingu,
- Serwery Archiwizacji,
- Macierz dyskowa

Zasilanie danymi systemu odbywa się poprzez dedykowane łącze w warstwie L2 przez które przesyłany jest obraz z kamer.

2.2. Wymagania ilościowe

Poniżej przestawiono wymagania infrastruktury IT.

lp.	*Nazwa*	*Ilość*
1.	Macierz dyskowa	1 szt.
2.	Serwer	3 szt.
4.	System backupu	1 komplet
5.	Zapora bezpieczeństwa sieciowego	1 komplet
6.	Przełączniki sieci LAN	1 komplet

2.3. Tabele parametrów techicznych

2.3.1. Macierz dyskowa

1. Zapytanie dotyczy dostarczenia systemu pamięci masowej składającego się z pojedynczej macierzy. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych połączonych przełącznikami SAN lub tak zwanym wirtualizatorem w sieci SAN.
2. Macierz powinna mieć możliwość instalacji w posiadanej przez Zamawiającego szafie Rack 19".
3. Wymagana przestrzeń dyskowa macierzy, co najmniej 100TB (przestrzeń efektywna, 1KB=1024B).
4. Przestrzeń dyskowa zbudowana w oparciu o 41 dysków 1200GB 10K SAS, 33 dyski 4TB 10K NL-SAS, 5 dysków 200GB SSD,
5. Wymagane jest, aby macierz wspierała różne poziomy zabezpieczeń RAID w tym, co najmniej RAID-10, RAID-5, RAID-6.

6. Wymagane jest, aby macierz obsługiwała, co najmniej następujące rodzaje dysków twardych: SAS-2 (300GB, 600GB, 1200GB), flash (400GB, 1.6TB, 3.2TB), SAS-NL lub SATA (4TB).
7. Wymagane jest, aby minimalnym kwantem rozbudowy ilości dysków w macierzy była jedna grupa dyskowa RAID, zbudowana w oparciu o nie więcej niż 8 dysków.
8. Oferowana macierz powinna posiadać możliwość rozbudowy do co najmniej 264 dysków.
9. Wymagane jest zapewnienie odpowiedniej ilości dysków zapasowych zgodnie z zaleceniami producenta macierzy.
10. Dostarczona macierz powinna posiadać możliwość zdefiniowania i udostępnienia serwerom co najmniej 4096 wolumenów logicznych bez konieczności dokupienia i instalacji dodatkowych licencji.
11. Macierz powinna umożliwiać utworzenie wolumenu logicznego o rozmiarze 60TB.
12. Macierz powinna posiadać funkcjonalność partycjonowania pamięci cache. Jeżeli funkcjonalność taka wymaga licencji to należy dostarczyć licencję umożliwiająca utworzenie co najmniej 8-śmiu partycji.
13. Macierz musi być wyposażona w co najmniej jedną parę redundantnych kontrolerów.
14. Kontrolery obsługujące dyski powinny być wyposażone w minimum 8 połączeń, co najmniej 12 Gbps SAS lub 16 połączeń, co najmniej 6 Gbps SAS . Wszystkie połączenia powinny być aktywne.
15. Macierz powinna być wyposażona w co najmniej 8 portów FC 8Gbps.
16. Wszystkie porty FC powinny być wyposażone w 8Gbps wkładki typu shortwave, multimode.
17. Nie dopuszcza się rozwiązania, w którym usługi protokołu Fiber Channel realizowane są w oparciu o emulację protokołu FC na wewnętrznym systemie plików macierzy dyskowej.
18. Wymagane jest, aby macierz wyposażona była w co najmniej 64 GB pamięci cache.
19. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci cache muszą być zabezpieczone metodą trwałego zapisu na dedykowany do tego celu dysk.
20. Macierz musi mieć możliwość wirtualizacji zasobów znajdujących się na innych macierzach dyskowych. Funkcjonalność wirtualizacji zewnętrznych zasobów dyskowych powinna być wbudowana w kontrolery macierzy. Funkcjonalność ta powinna być dostarczona z macierzą dyskową z licencją obejmującą nieograniczoną ilość wirtualizowanych TB przestrzeni dyskowej.
21. Macierz powinna posiadać możliwość definiowana wirtualnych wolumenów logicznych, których pojemność może być większa od rzeczywistej przestrzeni dyskowej skonfigurowanej w obrębie puli dysków twardych („thin provisioning"). Funkcjonalność „thin provisioning" powinna być dostarczona wraz z oferowaną macierzą z licencją na nieograniczoną pojemność dyskową.
22. Macierzy powinna posiadać możliwość dynamicznego i automatycznego relokowania fragmentów wolumenów logicznych pomiędzy co najmniej trzema różnymi klasami pamięci masowej („auto tiering"). Licencja na powyższą funkcjonalność jest przedmiotem zapytania.
23. Macierz powinna posiadać możliwość migracji całych wolumenów zarówno pomiędzy różnymi dyskami wewnątrz macierzy jak i pomiędzy różnymi zwirtualizowanymi macierzami. Migracja powinna odbywać się w sposób przeźroczysty dla aplikacji (online). Licencja na powyższą funkcjonalność nie jest przedmiotem zapytania.
24. Macierz powinna posiadać oprogramowanie do zarządzania macierzą, pozwalające na co *najmniej:*
    - Tworzenie i nazywanie wolumenów logicznych LUN
    - Mapowanie wolumenów logicznych do serwerów
    - Ustawianie priorytetu dla poszczególnych serwerów korzystających z przestrzeni dyskowej macierzy (zarówno pod względem ich przepustowości jak i obciążenia I/O)
    - Monitorowanie wykorzystywanej przestrzeni, efektywnej i surowej (RAW) macierzy.
25. Wymagane jest zaproponowanie dla oferowanej macierzy oprogramowania pozwalającego na monitorowanie i raportowanie wydajności poszczególnych komponentów macierzy, w tym co najmniej: procesorów, pamięci cache, wolumenów logicznych, grup dyskowych, portów zewnętrznych.
26. Wymagane jest zaproponowanie dla oferowanej macierzy oprogramowania do zarządzania wielościeżkowością (multipathing) i równoważeniem obciążeń (loadbalancing) dla co najmniej takich systemów jak: AIX, Linux, Windows, VMware. Musi istnieć możliwość monitorowania wszystkich ścieżek FC zarządzanych przez ww. oprogramowanie z wykorzystaniem jednej centralnej konsoli zarządzającej. Wymagana licencja na nieograniczoną ilość serwerów.
27. Macierz powinna posiadać możliwość wykonywania kopii pełnych typu klon i pozwalać na:
    - wykonywanie co najmniej 3 kopii pełnych dla pojedynczego wolumenu źródłowego.
    - re-synchronizację danych pomiędzy wolumenami źródłowym i kopią. Podczas wykonywania re-synchronizacji pomiędzy wolumenami kopiowane powinny być tylko dane różnicowe.

Licencja na powyższą funkcjonalność nie jest przedmiotem zapytania.

28. Macierz powinna posiadać możliwość wykonywania kopii migawkowych i pozwalać na wykonywanie co najmniej 1024 kopii migawkowych dla pojedynczego wolumenu źródłowego. Licencja na powyższą funkcjonalność nie jest przedmiotem zapytania.
29. Macierz powinna posiadać możliwość replikacji synchronicznej i asynchronicznej. Licencja na powyższą funkcjonalność nie jest przedmiotem zapytania.
30. Serwis w wymiarze 36-cio miesięcznym serwis 365/7/24. Wymagane jest pozostawienie uszkodzonych dysków u zamawiającego. Wymagana jest ciągłe monitorowanie pracy macierzy przez organizację serwisową producenta.
31. Wymagana dostawa 4 wkładek światłowodowych do przełącznika Brocade 300 w celu przyłączenia posiadanej przez Zamawiającego macierzy HP i udostępnienia jej zasobów z oferowanej macierzy.

2.3.2. Serwer

Komponent	Minimalne wymagania
Obudowa	Obudowa typu Rack o wysokości maksymalnej 2U, z możliwością instalacji do 8 dysków 2.5" HotPlug wraz kompletem szyn umożliwiających montaż w standardowej szafie Rack,
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Procesor	Dwa procesory dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku minimum 600 punktów w teście SPECint_rate_base2006 dostępnym na stronie internetowej www.spec.org dla konfiguracji dwuprocesorowej. Do oferty należy załączyć wynik testu dla oferowanego modelu serwera wraz z oferowanym modelem procesora.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Pamięć RAM	256 GB pamięci RAM typu LV RDIMM o częstotliwości pracy 2133MHz.
Sloty PCI Express	- minimum trzy sloty x16 generacji 3 o prędkości minimum x8
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024
Wbudowane porty	min. 2 portów USB z czego min. 1 w technologii 3.0 , 2 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232.
Interfejsy sieciowe	*Zainstalowane dodatkowo w złączach PCI Express karty sieciowe, posiadające łącznie min. 2 interfejsy 10Gb* SFP+ oraz 2 interfejsy FC 8Gbps
Zasilacze	Redundantne zasilacze Hot Plug wraz z kablami zasilającymi o dł. min. 2m każdy.
Wentylatory	redundantne wentylatory Hot-Plug
Bezpieczeństwo	- Elektroniczny panel informacyjny umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze, adresach MAC kart sieciowych, numerze serwisowym serwera, aktualnym zużyciu energii, nazwie serwera, modelu serwera. -Zintegrowany z płytą główną moduł TPM. -Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. - fabryczne oznaczenie urządzenia, wykonane przez producenta serwera informujące Zamawiającego m.in. o numerze serwisowym serwera, pełnej nazwie podmiotu Zamawiającego, modelu serwera; gwarantujące Zamawiającemu dostawę nowego, nieużywanego i nie pochodzącego z innych projektów sprzętu.
Karta zarządzająca	Niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płytą główną lub jako dodatkowa karta rozszerzeń (Zamawiający dopuszcza zastosowanie karty instalowanej w slocie PCI Express jednak nie może ona powodować zmniejszenia minimalnej ilości wymaganych slotów w serwerze), posiadająca minimalną funkcjonalność : - komunikacja poprzez interfejs RJ45 - podstawowe zarządzanie serwerem poprzez protokół IPMI 2.0, SNMP, VLAN tagging - wbudowana diagnostyka - wbudowane narzędzia do instalacji systemów operacyjnych - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń - monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji - lokalna oraz zdalna konfiguracja serwera - zdalna instalacja systemów operacyjnych - wsparcie dla IPv4 i IPv6 - zapis zrzutu ekranu z ostatniej awarii - możliwość zarządzania poprzez bezpośrednie podłączenie kablem do dedykowanego złącza USB - integracja z Active Directory Możliwość rozbudowy funkcjonalności karty o automatyczne przywracanie ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów z dedykowanej pamięci flash (w tym kontrolera RAID, kart sieciowych, płyty głównej).

Gwarancja	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany sewer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2008 R2 x64, x86, Microsoft Windows Server 2012 R2 Zainstalowany system Windows Serwer 2012,
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Oprogramowanie	System operacyjny Microsoft Windows HYPER-V
Instruktaż	Jeden instruktaż do wszystkich serwerów obejmujący zakresem: • Instalacja i konfiguracja Windows Server 2012. • Monitorowanie i utrzymywania serwerów Windows Server 2012. • Wykorzystanie Windows PowerShell 3.0 do zarządzania Windows Server 2012. • Konfiguracja magazynu w Windows Server 2012. • Wdrażanie i zarządzanie usługami sieciowymi. • *Wdrażanie i zarządzanie infrastrukturą DirectAccess.* • Dostarczanie wysoko dostępnych usług sieciowych i aplikacji z wykorzystaniem failover clustering. • Wdrażanie i konfiguracja maszyn wirtualnych na Hyper-V. • Wdrażanie i zarządzanie maszynami wirtualnymi w klastrze pracy awaryjnej. • Konfiguracja Dynamic Access Control do zarządzania i inspekcji dostępu do współdzielonych plików. • Implementacja nowych funkcji w Active Directory Domain Services (AD DS) dla Windows Server 2012. • Planowanie i wdrażanie Active Directory Federation Services (AD FS).

2.3.3. System backupu

1. Architektura centralna systemu backupu typu klient serwer,
2. Oprogramowanie powinno posiadać wsparcie dla backupu wykonywanego po sieci SAN oraz LAN,
3. Backup za pomocą agentów dla systemów operacyjnych Windows, Linux, MacOS, Solaris,
4. Backup baz danych przy pomocy agentów,
5. Możliwość konfiguracji backupów pełnych i przyrostowych,
6. Komplet licencji wymaganych do poprawnej pracy oprogramowania backupowego,
7. Wsparcie techniczne w okresie 3 lat,

2.3.4. Zapora bezpieczeństwa sieciowego

L.p.	Minimalne wymagania
1.	Zapora ogniowa czyli urządzenie klasy UTM musi zostać dostarczona jako jedno urządzenie lub powinien składać się z kilku połączonych urządzeń zapewniających wymagane funkcjonalność: - zapora ogniowa, - analizator logów bezpieczeństwa przyłączony do zapory ogniowej (UTM) przy pomocy złącza GbE, W przypadku zaoferowania kilku urządzeń wykonawca uwzględni w ofercie wszystkie niezbędne elementy zapewniające poprawną pracę takie jak moduły światłowodowe, okablowanie, niezbędne licencje.
2.	System ochrony UTM musi być zbudowany przy użyciu minimalnej ilości elementów ruchomych, krytycznych dla jego działania: brak magnetycznego twardego dysku; dopuszczalny dysk SSD lub pamięć FLASH. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanego układu ASIC. Minimalna pojemność przestrzeni dyskowej 60GB,
3.	Urządzenia ochronne UTM muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny powinny pochodzić od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie).

4.	Ilości złącz dla UTM - nie mniej niż 26 złącz w szczególności: • 12 złącz Ethernet 10/100/1000 Base-TX, • 8 złącz 1000 SFP, • 2 złącza na potrzeby zarządzania, • 2 złącza 10GbE SFP+ obsadzone wkładką światłowodową jedno modową (SM), • 2 pary złącz typu „bypass interface" zapewniające ciągłość działania połączenia w wyniku awarii zasilania,
5.	System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych: • kontrolę dostępu - zaporę bezpieczeństwa klasy Stateful Inspection • ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM) • poufność danych - IPSec VPN oraz SSL VPN • ochronę przed atakami - Intrusion Prevention System [IPS/IDS] oraz funkcjonalności uzupełniających: • kontrolę treści – Web Filter [WF] • kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) • kontrolę pasma oraz ruchu [QoS i Traffic shaping] • kontrolę komunikatorów sieciowych (IM) oraz aplikacji P2P
6.	Urządzenie UTM powinno dawać możliwość ustawienia jednego z dwóch trybów pracy: jako router/NAT (3.warstwa ISO-OSI) lub jako most /transparent bridge/ .
7.	Wykrywanie i blokowanie ataków (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. Nie mniej niż 4000 sygnatur ataków. Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie, wykrywanie anomalii protokołów i ruchu
8.	Wymagane funkcjonalności UTM: • Statyczna i dynamiczna translacja adresów (NAT). • Translacja NAPT.
9.	Definiowanie w jednym urządzeniu UTM bez dodatkowych licencji nie mniej niż 10 wirtualnych zapór bezpieczeństwa, gdzie każdy z nich posiada indywidualne ustawienia wszystkich funkcji bezpieczeństwa i dostęp administracyjny. Obsługa polityk rutingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego. Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM.
10.	Wymagane dla UTM nie mniej niż: Tworzenie połączeń w topologii Site-to-site oraz Client-to-site. Producent sprzętowej zapory bezpieczeństwa musi umożliwiać nieodpłatne pobranie klienta VPN własnej produkcji realizującego następujące mechanizmy ochrony: • firewall • antywirus • web filtering • antyspam Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności; Konfiguracja w oparciu o politykę bezpieczeństwa *(policy based VPN) i tabele routingu (interface based VPN); Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth*
11.	System UTM zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: • haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia • haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP • haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych Rozwiązanie powinno umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych.
12.	Obsługa nie mniej niż 7 000 000 jednoczesnych połączeń i 190 000 nowych połączeń na sekundę Przepływność nie mniejsza niż 20Gb/s dla ruchu nieszyfrowanego, Obsługa nie mniej niż 50 0000 jednoczesnych tuneli VPN. Przeputowość urządzenia dla AV– nie mniejsza niż 3000 Mb/s. Przeputowość urządzenia dla IPS – nie mniejsza niż 6Gb/s
13.	Monitoring i wykrywanie uszkodzenia elementów sprzętowych UTM i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive
14.	Konfiguracja UTM poprzez linię komend oraz wbudowaną konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą: • haseł statycznych • haseł dynamicznych (RADIUS, RSA SecureID) System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB. Jednocześnie, dla sprzętowej zapory bezpieczeństwa powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.
15.	Zasilanie UTM z sieci 230V/50Hz. Zasilacze wymieniane podczas pracy urzącenia,
16.	Obudowa UTM ma mieć możliwość zamontowania w szafie 19". Jeżeli wymagane są szyny montarzowe należy je uwzględnić w ofercie.
17.	Wymagane certyfikaty producenta oferowanej sprzętowej zapory bezpieczeństwa UTM: ISO 9001, UTM NSS Approved, EAL4+, ICSA Labs dla funkcji: Firewall, IPSec, SSL, Network IPS, Antywirus.
18.	Wymagane licencje (sygnatury) dla wszystkich dostępnych funkcji bezpieczeństwa na okres trzech lat,

	Elementy systemu bezpieczeństwa odpowiedzialne za zarządzanie i monitoring logów mają umożliwiać centralizację procesów zarządzania wszystkimi funkcjonalnościami elementów realizujących funkcje bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. W ramach systemu logowania i raportowania dostawca powinien dostarczyć spójny system monitorujący, gromadzący logi, korelujący zdarzenia i generujący raporty na podstawie danych ze wszystkich elementów systemu bezpieczeństwa. Platforma powinna dysponować predefiniowanym zestawem przykładów raportów, dla których administrator systemu będzie mógł modyfikować parametry prezentowania wyników. System centralnego logowania i raportowania powinien być dostarczony w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
19.	W ramach centralnego systemu logowania, raportowania i korelacji powinny być realizowane przynajmniej poniższe funkcjonalności: 1. Konfigurowalne opcje powiadamiania o zdarzeniach jak. email, SNMP 2. Podgląd logowanych zdarzeń w czasie rzeczywistym. 3. Możliwość generowania raportów w zakresie wszystkich funkcjonalności bezpieczeństwa realizowanych przez system - na żądanie oraz w trybie cyklicznym, w postaci dokumentów PDF. Raporty powinny obejmować zagadnienie dotyczące całej sfery bezpieczeństwa. 4. Zastosowane systemy logowania powinny umożliwiać cykliczny eksport zgromadzonych logów do zewnętrznych systemów przechowywania danych w celu ich długo czasowego składowania. 5. Na podstawie analizy przeprowadzonych testów w zakresie ilości logów w ciągu sekundy, zastosowany system centralnego logowania powinien umożliwiać zapis oraz analizę co najmniej 300 nowych logów/sekundę. 6. System powinien dysponować co najmniej 4 interfejsami Ethernet 10/100/1000 oraz powierzchnią dyskową min. 1 TB

20.	Do urządzenia UTM należy dostarczyć autoryzowany przez producenta instruktarz w wymiarze min 2 dni roboczych dla dwóch administratorów. Minimalny zakres instruktarzu: 1. Wstęp do UTM a. podstawowa konfiguracja urządzenia UTM 2. Logowanie i monitoring a. konfiguracja logowania dla zdarzeń systemowych b. konfiguracja logowania ruchu c. alerty 3. Konfiguracja polityk firewalla a. zasada działania firewalla stanowego b. polityki firewalla c. reguły uwierzytelniające użytkowników d. polityki bazujące na urządzeniach e. NAT f. tworzenie obiektów dla reguł zapory ogniowej g. ochrona przed zagrożeniami – konfiguracja UTM h. traffic shaping 4. Lokalne uwierzytelnianie użytkowników a. metody uwierzytelniania b. obiekty użytkowników i grup c. dwuskładnikowe uwierzytelnianie 5. SSL-VPN a. koncepcja sieci VPN b. dostępne technologie c. architektura SSL VPN d. tryby działania SSL- VPN e. konfiguracja SSL-VPN 6. Wstęp do IPSec-VPN a. architektura b. topologie i konfiguracja IPSec VPN c. tryby pracy: route-based i policy-based 7. Skanowanie antywirusowe a. Conserve Mode b. skanowanie Proxy-Based c. skanowanie Flow-Based d. konfiguracja profilu AV e. kwarantanna f. globalne ustawienia modułu AV 8. Filtracja Antyspamowa a. metody filtrowania spamu b. Email Filtering c. obsługa nagłówków MIME d. konfiguracja czarnych i białych list e. DNS Blackholing i Open Relay Database 9. Filtr stron WWW a. metody filtrowania stron WWW b. kolejność filtrowania c. konfiguracja lokalnego filtra stron WWW d. filtrowanie po zawartości stron e. filtrowanie po kategoriach tematycznych 10. Kontrola aplikacji a. zasada działania i możliwości b. konfiguracja listy kontrolowanych aplikacji

2.3.5. Przełączniki sieci LAN,

2.3.5.1. Przełącznik 10GbE,

1. Przełącznik musi być dedykowanym urządzeniem sieciowym o przystosowanym do montowania w szafie rack.
2. Przełącznik musi posiadać wbudowane nie mniej niż 48 portów dostępowych przeznaczonych na moduły 1/10 Gigabit Ethernet.
3. Przełącznik musi posiadać nie mniej niż 6 portów uplink 40 Gigabit Ethernet. Wszystkie porty 10 Gigabit Ethernet i 40 Gigabit Ethernet muszą jednocześnie być aktywnie i aktywnie przesyłać ruch użytkowników. Musi istnieć możliwość konwersji każdego portu 40 Gigabit Ethernet do 4 portów 10 Gigabit Ethernet.

4. Urządzenie musi posiadać możliwość pracy jako część (karta liniowa) wirtualnego przełącznika składającego się z innych urządzeń tego samego producenta. Wirtualny przełącznik z punktu widzenia zarządzania oraz innych urządzeń w sieci musi być widoczny jako jedno urządzenie. Wirtualny przełącznik musi być odporny na awarie, tzn. zarządzanie oraz wszelkie połączenia kontrolne muszą być zdublowane. Do połączenia w strukturę wirtualnego przełącznika muszą być wykorzystane nie mniej niż 2 porty uplink 40 Gigabit Ethernet przełącznika fizycznego. Wirtualny przełącznik musi pozwalać na rozbudowę do nie mniej niż 30 fizycznych przełączników i sumarycznie nie mniej niż 768 portów 10 Gigabit Ethernet.
5. Urządzenie musi obsługiwać moduły SFP Gigabit Ethernet nie mniej 1000Base-T, SX, LX. Producent musi dopuszczać możliwość wykorzystywania modułów SFP pochodzących od innych producentów.
6. Urządzenie musi obsługiwać moduły SFP+ 10 Gigabit Ethernet nie mniej niż SR, USR, LR, ER. Ponadto urządzenie musi obsługiwać moduły miedziane (Direct Attach Copper) do zestawienia połączeń 10 Gigabit Ethernet. Producent musi dopuszczać możliwość wykorzystywania modułów SFP+ pochodzących od innych producentów.
7. Urządzenie musi obsługiwać moduły QSFP+ 40 Gigabit Ethernet nie mniej niż SR, LR oraz moduły miedziane (Direct Attach Copper).
8. Przełącznik musi być dostarczony z 18 modułami SFP+ 10 Gigabit Ethernet SR
9. Przełącznik musi posiadać wymienne zasilacze AC. Urządzenie musi być wyposażone w redundantne źródło zasilania. Urządzenie musi posiadać wymienny moduł wentylacji.
10. Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
11. Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh.
12. Przełącznik musi posiadać architekturę non-blocking. Zagregowana wydajność przełączania w warstwie 2 nie może być niższa niż 1.4 Tb/s. Urządzenie musi obsługiwać nie mniej niż 960 milionów ramek/sekundę. Przełącznik nie może obsługiwać mniej niż 250 000 adresów MAC. Urządzenie musi obsługiwać tryby przełączania ramek store-and-forward oraz cut-through.
13. Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
14. Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4000.
15. Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 120 grup LAG, po nie mniej niż 32 porty. Przełącznik musi obsługiwać funkcję typu Multi-chassis LAG w celu zestawiania połączeń zagregowanych zaterminowanych na niezależnych przełącznikach fizycznych.
16. Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003.
17. Przełącznik musi obsługiwać protokół LLDP.
18. Urządzenie musi obsługiwać ruting między sieciami VLAN – ruting statyczny, oraz protokoły rutingu dynamicznego: RIP, OSPF. Musi istnieć możliwość uruchomienia protokołów IS-IS, BGP oraz MPLS (w tym L3 VPN oraz LDP i RSVP) poprzez zakup dedykowanej licencji. Urządzenie musi obsługiwać protokoły rutingu multicast, nie mniej niż IGMP (v1, v2, v3), PIM-SM oraz PIM-SSM.
19. Przełącznik musi obsługiwać mechanizm wykrywania awarii BFD, oraz pozwalać na stworzenie konfiguracji HA z wykorzystaniem protokołu VRRP.
20. Przełącznik musi umożliwiać aktualizację oprogramowania przy zachowaniu ciągłości pracy i stanu protokołów routingu i przełączania (In Service Software Upgrade). Do realizacji tej funkcji wymagany jest zapasowy moduł kontrolny realizowany sprzętowo lub jako maszyna wirtualna.
21. Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek dla ruchu unicast.
22. Urządzenie musi obsługiwać filtrowanie ruchu na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Filtrowanie ruchu musi być realizowane sprzętowo. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
23. Przełącznik musi obsługiwać limitowanie adresów MAC.

24. Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3) oraz grupy RMON. Musi być dostępna funkcja kopiowania (mirroring) ruchu.
25. W celu integracji z sieciami storage urządzenie musi obsługiwać funkcje: FIP Snooping, Data Center Bridging Capability Exchange (DCBX) oraz Priority-based Flow Control (PFC). Przełącznik musi pozwalać na uruchomienie jako przełącznik tranzytowy FCoE.
26. Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu rutingu IP, odpowiedzialnego za ustalanie tras rutingu i zarządzanie urządzeniem.
27. Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 20 poprzednich, kompletnych konfiguracji.
28. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim.
29. Autoryzowane szkolenia dla jednego administrator w języku Polskim.

2.3.5.2. Przełącznik GbE typ 1,

1. Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie rack.
2. Przełącznik musi posiadać 24 portów dostępowych Ethernet 10/100/1000 Auto-MDI/MDIX.
3. Wszystkie porty dostępowe muszą obsługiwać standard 802.3af (Power over Ethernet) oraz 802.at (Power over Ethernet+). Przełącznik musi udostępniać 15.4 W na każdym porcie dostępowym jednocześnie.
4. Przełącznik musi posiadać nie mniej niż 4 porty uplink 10 Gigabit Ethernet SFP+. Korzystanie z portów uplink nie może powodować wyłączenia portów dostępowych 10/100/1000. Porty uplink muszą akceptować również wkładki SFP umożliwiając obsługę połączeń uplink Gigabit Ethernet. Przełącznik musi być dostarczony z 2 wkładkami 10GbE SR.
5. Przełącznik musi umożliwiać stworzenie stosu (w postaci pętli) liczącego nie mniej niż 10 urządzeń. Dopuszczalne jest podłączanie do stosu portami uplink 10 Gb/s. Stos musi być widoczny z punktu widzenia zarządzania oraz innych urządzeń sieciowych jako jedno urządzenie. Zarządzanie wszystkimi przełącznikami w stosie musi się odbywać z dowolnego przełącznika będącego częścią stosu. Stos musi być odporny na awarie, tzn. przełącznik kontrolujący pracę stosu (master) musi być automatycznie zastąpiony przełącznikiem pełniącym rolę backup'u – wybór przełącznika backup nie może odbywać się w momencie awarii przełącznika master.
6. Przełącznik musi posiadać wbudowany zasilacz AC. Urządzenie musi posiadać wentylator – z przepływem powietrza od przodu do tyłu. Urządzenie musi posiadać panel LCD z przyciskami, pozwalający na wykonywanie podstawowych czynności związanych z zarządzaniem (adresacja IP, reset). Musi istnieć możliwość podłączenia zewnętrznego redundantnego źródła zasilania.
7. Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
8. Przełącznik musi być wyposażony w nie mniej niż 1 GB pamięci Flash oraz 1 GB pamięci DRAM.
9. Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.
10. Przełącznik musi posiadać architekturę non-blocking. Wydajność przełączania w warstwie 2 nie może być niższa niż 120 Gb/s i 90 milionów pakietów na sekundę. Przełącznik nie może obsługiwać mniej niż 16 000 adresów MAC.
11. Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
12. Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4096. Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based). W celu automatycznej konfiguracji sieci VLAN, przełącznik musi obsługiwać protokół MVRP.
13. Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 32 grupy LAG, po nie mniej niż 8 portów.
14. Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, zgodnie z IEEE 802.1D i 802.1w, a także Multiple Spanning Tree zgodnie z IEEE 802.1s (nie mniej niż 64 instancje MSTP).
15. Przełącznik musi obsługiwać protokół LLDP i LLDP-MED.
16. Urządzenie musi obsługiwać ruting między sieciami VLAN – ruting statyczny, oraz protokół rutingu dynamicznego RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 8

000. Urządzenie musi posiadać funkcję IGMP Snooping (v1, v2, v3). Urządzenie musi pozwalać na zarządzanie po IPv6.

17. Urządzenie musi posiadać mechanizmy priorytetyzowania dla ruchu wchodzącego i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.
18. Urządzenie musi obsługiwać filtrowanie ruchu na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo nie mniej niż 1500 reguł filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
19. Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping.
20. Przełącznik musi obsługiwać IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. Przełącznik musi obsługiwać co najmniej następujące typy EAP: MD5, TLS, TTLS, PEAP.
21. Urządzenie musi obsługiwać protokół SNMP (wersje 2 i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
22. Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu rutingu IP, odpowiedzialnego za ustalanie tras rutingu i zarządzanie urządzeniem.
23. Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 20 poprzednich, kompletnych konfiguracji.
24. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim.

2.3.5.3. Przełącznik GbE typ 2,

1. Dedykowane urządzenie sieciowe o wysokości 1U przystosowane do montowania w szafie rack.
2. 48 porty dostępowe Ethernet 10/100/1000 Auto-MDI/MDIX.
3. Wyposażony w nie mniej niż 4 porty uplink 10 Gigabit Ethernet SFP+ lub XFP. Wszystkie porty dostępowe 10/100/1000 muszą być aktywne po wyposażeniu przełącznika w moduł uplink. W przypadku SFP+, porty uplink muszą akceptować również wkładki SFP, umożliwiając obsługę połączeń uplink Gigabit Ethernet. Przełącznik musi być dostarczony z 2 wkładkami 10GbE SR.
4. Możliwość stworzenia stosu (w postaci pętli) liczącego nie mniej niż 10 urządzeń. Dopuszczalne jest podłączanie do stosu portami uplink 10 Gb/s. Stos jest widoczny z punktu widzenia zarządzania oraz innych urządzeń sieciowych jako jedno urządzenie. Zarządzanie wszystkimi przełącznikami w stosie odbywa się z dowolnego przełącznika będącego częścią stosu. Stos jest odporny na awarie, tzn. przełącznik kontrolujący pracę stosu (master) w razie jego awarii, jest automatycznie zastąpiony przełącznikiem pełniącym rolę master backup'u.
5. Przełącznik musi posiadać wbudowany zasilacz AC. Urządzenie musi posiadać wentylator – z przepływem powietrza od przodu do tyłu. Urządzenie musi posiadać panel LCD z przyciskami, pozwalający na wykonywanie podstawowych czynności związanych z zarządzaniem (adresacja IP, reset). Musi istnieć możliwość podłączenia zewnętrznego redundantnego źródła zasilania.
6. Posiada port konsoli oraz dedykowany interfejs Ethernet do zarządzania out-of-band.
7. Zarządzanie za pośrednictwem interfejsu linii komend (CLI) poprzez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.
8. Architektura non-blocking. Wydajność przełączania w warstwie 2 nie niższa niż 170 Gb/s i 125 milionów pakietów na sekundę. Obsługa nie mniej niż 16 000 adresów MAC.
9. Obsługa ramek Jumbo (9kb).
10. Obsługa sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4094. Obsługa sieci VLAN opartej o porty fizyczne (port-based) i adresy MAC (MAC-based).
11. Obsługa agregowania połączeń zgodne z IEEE 802.3ad.

12. Obsługa protokołu Spanning Tree i Rapid Spannig Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2005.
13. Obsługa protokółu LLDP i LLDP-MED lub odpowiadającego.
14. Obsługa rutingu między sieciami VLAN – rutingu statycznego, oraz protokołu rutingu dynamicznego RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 8000.
15. Obsługa IGMP snooping (v1,v2,v3)
16. Zarządzanie po IPv6
17. Mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Sprzętowa obsługa nie mniej niż 8 kolejek na port fizyczny.
18. Obsługa filtrowania ruchu co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów w regułach filtrowania ruchu. Funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
19. Obsługa mechanizmów bezpieczeństwa typu limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping.
20. Obsługa IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przypisywanie ustawień dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS (co najmniej VLAN oraz reguła filtrowania ruchu). Możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. Obsługa co najmniej następujących typów EAP: MD5, TLS, TTLS, PEAP.
21. Obsługa protokołu SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
22. Architektura systemu operacyjnego urządzenia o budowie modularnej (poszczególne moduły działają w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów jest oddzielony od modułu rutingu IP, odpowiedzialnego za ustalanie tras rutingu i zarządzanie urządzeniem.
23. Mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji.
24. Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przez okres 3 lat. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta lub autoryzowanego dystrybutora sprzętu w języku polskim, możliwość zgłaszania problemów technicznych w dedykowanym systemie wsparcia online w trybie 24/7/365 opartym o interfejs webowy w języku polskim, wymianę uszkodzonego sprzętu (producent wysyła sprzęt następnego dnia roboczego), dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

3. Dostawa elementów serwerowni

3.1. Ogólny opis zamówienia

Celem Zamówienia jest dostawa infrastruktury na potrzeby pracy Systemów projektu SAVA. *Wyróżniamy następujące elementy wypoasrzenia serwerowni:*

- Klimatyzacja,
- Szafy RACK,
- Zasilanie Awaryjne UPS,
- Panele dystrybucji zasilania PDU,

Wymagania ilościowe dostawy elementów serwerowni:

lp.	Nazwa	Ilość
1.	*Klimatyzacja*	2 szt.
2.	Szafa RACK	2 szt.
4.	Zasilacz UPS	1 szt.
4.	Panele Dystrybucji Zasilania	4 szt.

3.2. Tabele parametrów technicznych

3.2.1. Wymagania dla szaf serwerowych RACK

1. Ilość 2 szt.,
2. Wymiary maksymalne szaf: 800x1200x2000mm (szerokość x głębokość x wysokość).
3. Wysokość użytkowa min. 42U, szerokość użytkowa 19-cali.
4. Obciążenie statyczne szafy min. 800 kg.
5. Konstrukcja szafy z profili stalowych spawanych.
6. Drzwi frontowe i tylne z blachy perforowanej, perforacja minimum 80% powierzchni.
7. Przepusty kablowe z dołu i od góry.

3.2.2. Wymagania dla zasilaczy awaryjnych UPS

1. Ilość: 1 szt.,
2. Zasilacz awaryjny UPS o mocy 6kVA 230V z czasem podtrzymania 15 min.
3. Opcjonalnie dodatkowy moduł baterii.
4. Obudowa w standardzie RACK 19-cali.
5. Tryb pracy „On-Line".
6. Parametry elektryczne:
    - napięcie wejściowe 230 V, tolerancja 200-284 V okablowanie 1P+N+PE
    - napięcie wyjściowe 230 V, tolerancja 200-284 V okablowanie 1P+N+PE
    - częstotliwość wejścia 50 (60) Hz
    - częstotliwość wyjścia 50 (60) Hz
7. Panel operatora wbudowany na płycie czołowej zawierający:

- Kontrolki LED,
- Przyciski sterowania.

8. Komunikacja i sygnalizacja:
   - Karta komunikacyjna SNMP,
   - Komunikacja stykowa.
9. W ramach dostawy zawarte mają być:
   - dostawa urządzeń o podanych parametrach na miejsce instalacji,
   - przeszkolenie obsługi pod względem prawidłowej eksploatacji,
   - dokumentacja w języku polskim,
   - montaż, uruchomienie, test prawidłowego działania systemu pod sztucznym obciążeniem min. 60% mocy znamionowej,
   - pełna dokumentacja urządzeń wraz ze stanowiskową, skróconą instrukcją obsługi
10. Dostawca urządzeń musi zapewnić gwarancję posprzedażną na okres 2 lat od daty dostawy oraz czas reakcji (rozpoczęcia prac mających na celu usunięcie awarii) wynoszący nie dłużej niż 8h od terminu zgłoszenia awarii przez Użytkownika.

3.2.3. Wymagania dla klimatyzacji

1. Ilość 2 szt.,
2. Wymagania dla układu klimatyzacji:
   - wydajność minimalna 10.0 kW,
   - zasilanie 230V/50Hz,
   - klasa energetyczna A,
   - montaż ścienny,
   - tryb pracy chłodzenie lub wentylacja, wentylator 2-biegowy,
   - pompka skroplin.
3. Wymagania dla instalacji czynnika chłodniczego:
   - długości instalacji min. 20m
   - różnica wysokości min. 10m
   - czynnik chłodniczy R-410A.
4. W ramach dostawy zawarte mają być:
   - dostawa urządzeń o podanych parametrach na miejsce instalacji,
   - przeszkolenie obsługi pod względem prawidłowej eksploatacji,
   - dokumentacja w języku polskim,
   - montaż, uruchomienie, test prawidłowego działania systemu pod sztucznym obciążeniem min. 60% mocy znamionowej,
   - pełna dokumentacja urządzeń wraz ze stanowiskową, skróconą instrukcją obsługi
5. Dostawca urządzeń musi zapewnić gwarancję posprzedażną na okres 2 lat od daty dostawy oraz czas reakcji (rozpoczęcia prac mających na celu usunięcie awarii) wynoszący nie dłużej niż 8h od terminu zgłoszenia awarii przez Użytkownika.

3.2.4. Wymagania dla paneli dystrybucji zasilania

1. Ilość 4 szt.,
2. Zasilanie 1-fazowe 230V, prąd znamionowy (fazowy) 16A.
3. Gniazda wyjściowe IEC 13, ilość gniazd minimum 6x2PZ.
4. Kabel zasilający do szafy giętki w izolacji PCV, 3-żyłowy, żyła miedziana, napięcie izolacji 0,75kV.
5. Uchwyty montażowe do szafy RACK.

4. Przystosowanie pomieszczeń serwerowni

4.1. Ogólny opis zamówienia

Przedmiotem zamówienia jest modernizacja i dostosowanie istniejącego pomieszczenia *technicznego do wymagań stawianych dla Centrum Przetwarzania Danych (CPD) i rozbudowa* okablowania strukturalnego LAN do istniejących punktów dystrybucyjnych.

4.2. Informacje ogólne

Na potrzeby budowy w/w infrastruktury teleinformatycznej planuje się adaptację i wyposażenie w niezbędne urządzenia i instalacje pomieszczenia serwerowni.

Aktualnie pomieszczenie przewidziane na Centrum Przetwarzania Danych (CPD) pełni funkcję pomieszczenia technicznego i nie zmieni swojego przeznaczenia.

W odległości do 80m znajduje się rozdzielnia elektryczna z niezbędnym zapasem mocy 20 kW, węzeł sieci LAN (GPD) i istniejące punkty dystrybucyjne (PD) w ilości 12 pkt. do których należy wykonać korespondencje światłowodowe znajdują siew średniej odległości do 280m każdy punkt PD i GPD.

W czasie prac instalacyjno-adaptacyjnych musi być zachowana ciągłość pracy istniejącej infrastruktury teleinformatycznej IT poprzez tymczasową redundancję łączy fizycznych i migrację sprzętu wraz z usługami pomiędzy adoptowanym pomieszczeniem a innymi punktami dostępowymi (pomieszczeniami IT) wskazanymi w trakcie realizacji przedmiotu zamówienia.

Pomieszczenie CPD wymaga adaptacji w zakresie ogólnobudowlanym a w szczególności:

- Wzmocnienie posadzki zależnie od oceny stanu technicznego.
- Wymiana drzwi wejściowych (1 szt.)
- Uzupełnienie ubytków i malowanie ścian (1 kpl).
- Żaluzje antywłamaniowe wewnętrze na oknach (1 szt) .
- Podłoga techniczna (podniesiona) (30 m2).
- Instalacja oświetlenia ogólnego i awaryjnego (1 kpl).
- Instalacja gniazd serwisowych 230V i LAN (2 pkt).
- Instalacja uziemienia i połączeń wyrównawczych (1 kpl).

Pomieszczenie CPD należy wyposażyć w dedykowane instalacje i urządzenia a w szczególności:

- Budowa przyłącza zasilającego 230/400V 20kW z zasilaczem awaryjnym UPS w tym rozdzielnie do zasilania szaf RACK i klimatyzacji (1 kpl).
- Klimatyzacja w układzie redundantnym (2 kpl).
- Szafy serwerowe w standardzie RACK 19-cali (2 szt).
- Listwy zasilające PDU (4 szt.).
- System okablowania strukturalnego LAN (1 kpl).
- System sygnalizacji pożaru (1 kpl).
- System gaszenia aerozolem (1 kpl).

- Systemy monitoringu wizyjnego (2 kamery).
- System kontroli dostępu (1 przejście).

Przedmiotowe opracowanie należy traktować jako specyfikację minimalnych parametrów technicznych materiałów i urządzeń do projektu wykonawczego z tym że nadrzędne stanowią obowiązujące przepisy prawa budowlanego i warunki techniczne wykonania i odbioru robót.

4.3. Szczegółowe uwarunkowania wykonania

Przedmiotem zadania jest wykonanie dokumentacji projektowej (budowlanej jeżeli wymagana i wykonawczej) oraz wszystkich prac budowlanych i instalacyjnych wraz z dostawą materiałów i urządzeń do modernizacji serwerowni. Zadanie obejmować będzie kompleksową realizację, „pod klucz", składającą się z następujących etapów procesu inwestycyjnego:

- Opracowanie dokumentacji projektowej w zakresie wyspecyfikowanym w Opisie Przedmiotu Zamówienia oraz uzyskanie akceptacji Zamawiającego.
- Wykonanie prac przygotowawczych i demontażowych jeżeli wymagane w pomieszczeniach objętych modernizacją.
- Wykonanie prac remontowo-budowlanych w zakresie wymienionym w Opisie Przedmiotu Zamówienia.
- Wykonanie prac instalacyjnych w zakresie wymienionym w Opisie Przedmiotu Zamówienia.
- Dostawa materiałów i urządzeń niezbędnych do wykonania przedmiotu zamówienia.
- Uruchomienie urządzeń oraz wykonanie testów, pomiarów i badań sprawdzających współdziałanie wszystkich zainstalowanych elementów w tym współpraca z istniejącą infrastrukturą IT.
- Przeprowadzenie szkoleń personelu wskazanego przez Zamawiającego.
- Opracowanie dokumentacji powykonawczej w tym instrukcji obsługi i harmonogramu przeglądów serwisowych i gwarancyjnych.
- Realizacja przeglądów serwisowych i gwarancyjnych przez okres 2 lat w/g opracowanego harmonogramu na koszt Wykonawcy włącznie z materiałami eksploatacyjnymi.

4.4. Dokumentacja projektowa

Dokumentacja powinna zawierać:

- Projekt zagospodarowania serwerowni.
- Projekt zasilania energetycznego.
- Projekt klimatyzacji.
- Projekt systemu detekcji pożaru i gaszenia aerozolem.
- Projekt elektronicznych systemów zabezpieczeń.
- Projekt okablowania strukturalnego.
- Harmonogram prac.

Dokumentację należy opracować zgodnie z ustawą z dnia 7 lipca 1994 – Prawo Budowlane (t.j. Dz. U. z 2010 r. nr 243 poz. 1623) oraz warunkami technicznymi wykonania i odbioru robót.

Każda część dokumentacji powinna być podpisana przez projektanta z właściwymi uprawnieniami budowlanymi dla danej branży.

Kompletną dokumentację projektową wraz z harmonogramem należy przedłożyć do zatwierdzenia. Wszystkie prace budowlano-instalacyjne prowadzone będą zgodnie z zatwierdzoną do realizacji dokumentacją projektową i harmonogramem.

Przedmiotową Opis Przedmiotu Zamówienia (OPZ) należy traktować jako zbiór założeń funkcjonalnych i minimalnych parametrów technicznych.

Całość zamówienia realizowana w trybie zaprojektuj i buduj „pod klucz", podany zakres ilościowy należy traktować jako orientacyjny i nie może stanowić podstawy do późniejszych roszczeń finansowych Wykonawcy.

4.5. Prace budowlane

Szczegółowe uwarunkowania robót budowlanych:

- Zakres robót budowlanych szczególnie uciążliwych w czynnych budynkach należy prowadzić w godzinach nocnych i dniach wolnych od pracy po wcześniejszym uzgodnieniu z administracją obiektu.
- Zakres prac w czynnych pomieszczeniach technicznych w czasie pracy urządzeń lub wymagający wyłączenia urządzeń należy wykonywać tylko i wyłącznie po wcześniejszym uzgodnieniu harmonogramu prac i pod nadzorem służb administracyjno-technicznych i Wykonawcy w przypadku ingerencji w zakres objęty gwarancją Wykonawcy lub dostawcy.
- Prowadzenie prac po godzinach pracy obiektu tylko po wcześniejszym uzgodnieniu z Zamawiającym i pod nadzorem administracji obiektu.
- Wykonawca zobowiązany jest do przedłożenia kart materiałowych użytych materiałów do akceptacji przez Zamawiającego przed ich zabudowaniem.
- Wykonawca ponosi całkowitą odpowiedzialność za prowadzenie robót zgodnie z umową, dokumentacją projektową, specyfikacją techniczną urządzeń, uzgodnionym harmonogramem prac oraz za jakość użytych materiałów i wykonanych robót.
- Wykonawca ponosi całkowitą odpowiedzialność cywilno-prawną za szkody wynikłe z zaniechania i niedbalstwa, działania niezgodne ze sztuką budowlaną i obowiązującymi przepisami oraz za niewłaściwe zabezpieczenie miejsca realizacji przedmiotu zamówienia.
- Wykonawca będzie odpowiadał za powierzone do adaptacji pomieszczenia oraz wszystkie materiały i elementy wyposażenia użyte do realizacji zadania od chwili protokolarnego przekazania pomieszczeń do adaptacji aż do odbioru końcowego.

4.6. Dokumentacja powykonawcza

Po zakończeniu prac budowlano-instalacyjnych Wykonawca zobowiązany jest do wykonania dokumentacji powykonawczej która powinna zawierać:

- Dokumentację rysunkową z opisem technicznym wykonanego zakresu prac.
- Dokumentację jakościową z wykazem użytych materiałów z podaniem nazw i producentów, wymaganych atestów, zezwoleń do użycia na terenie Polski itp.

- Protokoły z pomiarów i uruchomień w tym protokoły odbiorów technicznych i z pracy próbnej 48-godzinnej w ruchu ciągłym.
- Instrukcje obsługi i eksploatacji urządzeń.
- Harmonogram przeglądów serwisowych i gwarancyjnych.

Dokumentacja powykonawcza powinna dodatkowo zawierać informacje o wszystkich odstępstwach i zmianach w stosunku do projektu wykonawczego.

Zgodnie z zasadami zamówień publicznych Wykonawca może zastosować materiały i rozwiązania równoważne to jest w żadnym stopniu nieobniżające standardu i niezmieniające funkcjonalności przyjętej w Koncepcji i Specyfikacji Technicznej.

4.7. Tabele parametrów technicznych

4.7.1. Wymagania dla przegród budowlanych

1. *Ściany i stropy w klasie odporności ogniowej minimum 60 min.*
2. Średnice przepustów dobrane do wiązki kablowej lub rury instalacyjnej z zapasem minimum 20%, minimalna średnica 18mm.
3. Uszczelnienie przepustów kablowych masą ogniochronną o konsystencji pianki umożliwiającej późniejsze dołożenie kabli bez konieczności rozbierania całej przegrody. Klasa odporności ogniowej uszczelnień jak odporność ogniowa ściany przez którą przechodzi.
4. Zabezpieczenie przepustów rurowych przez ściany/stropy zewnętrzne szczelnymi kołnierzami uszczelniającymi na rurach.
5. Ściany malowane farbami zmywalnymi, kolor biały.

4.7.2. Wymagania dla posadzek

1. Ilość 30m2,
2. Nośność posadzki min. 1000 kg/m2.
3. Nawierzchnia gładka, antystatyczna zabezpieczona przed pyleniem.

4.7.3. Wymagania dla podłogi technicznej

1. Ilość 30m2,
2. Wysokość przestrzeni pod podłogą techniczną minimum 250mm.
3. Podłoga w całości demontowalna przy drzwiach wejściowych pochylnia do transportu urządzeń.
4. Panel podłogi wykonany z materiału niezapalnego od strony spodniej i trudnozapalnego od strony wierzchniej, klasa odporności ogniowej EI-30.
5. System uchwytów umożliwiających montaż koryt kablowych do elementów konstrukcyjnych podłogi.
6. Płyty podłogowe wiórowe o gęstości min. 700 kg/m3 o wymiarach 600x600x40mm z wykończeniem wierzchnim wykładziną antyelektrostatyczną PCV jasnoszarą, spodnim z blachy stalowej ocynkowanej ogniowo o grubości min. 0,5mm o obciążalności podłogi min. 1000 kg/m2.
7. Wsporniki stalowe wolnostojące o płynnie regulowanej wysokości, ocynkowane galwanicznie, połączone trawersami, nakładki tłumiące PCV, przewodzące o oporności upływu Ru >5x104.