Załącznik nr 1 do Ogłoszenia

Część 1: Przełączniki sieci Ethernet – 8 szt.

Opis ogólny

GigabitSwitch 48 portów STACK 10 Gb z PoE	48 portowy gigabitowy przełącznik ethernetowy o stałej konfiguracji z możliwością pracy w stosie (STACK nie mniej niż 10 Gb/s) z PoE przeznaczony do szafy dostępowej. W zestawie komplet miniGBIC (mini Gigabit Interface Converter – konwerter gigabitowego interfejsu) - 2 szt. miniGBIC.	1 szt.
GigabitSwitch 48 portów STACK 10 Gb bez PoE	48 portowy gigabitowy przełącznik ethernetowy o stałej konfiguracji z możliwością pracy w stosie (STACK niemniej niż 10 Gb/s) bez PoE przeznaczony do szafy dostępowej. W zestawie komplet miniGBIC (mini Gigabit Interface Converter – konwerter gigabitowego interfejsu) 2 szt. miniGBIC do każdego switcha.	4 szt.
GigabitSwitch 48 portów STACK 40 Gb bez PoE	48 portowy przełącznik ethernetowy o stałej konfiguracji z możliwością pracy w stosie ze STACK 40 Gb/s bez PoE przeznaczony do szafy serwerowej. W zestawie komplet miniGBIC (mini Gigabit Interface Converter – konwerter gigabitowego interfejsu) 2 szt. miniGBIC do każdego switcha.	3 szt.

Wszystkie przełączniki muszą pochodzić od jednego producenta.

Minimalne wymagania techniczne dla: GigabitSwitch 48 portów (STACK 10 Gb) z PoE

- Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie rack.
- Przełącznik musi posiadać 48 portów dostępowych Ethernet 10/100/1000 Auto-MDI/MDIX zgodnych z PoE+ 802.3at (30W). Moc zasilacza przeznaczona na realizacje funkcji PoE nie może być mniejsza niż 740W.
- 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. Wymiana modułu uplink nie może wymagać wyłączenia przełącznika. Porty uplink muszą akceptować również wkładki SFP umożliwiając obsługę połączeń uplink Gigabit Ethernet.
- 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. Przełączniki pracujące w stosie, pełniące role control plane, muszą posiadać funkcje synchronizacji stanów protokołów L2 i L3, tablic routingu oraz tablic forwardingu.
- 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).
- Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
- Przełącznik musi być wyposażony w nie mniej niż 1 GB pamięci Flash oraz 1 GB pamięci DRAM.
- Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.
- Przełącznik musi posiadać architekturę non-blocking. Wydajność przełączania w warstwie 2 nie może być niższa niż 175 Gb/s i 130 milionów pakietów na sekundę. Przełącznik nie może obsługiwać mniej niż 16 000 adresów MAC.
- Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).

Załącznik nr 1 do Ogłoszenia

- Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4000. 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.
- Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 32 grupy LAG, po nie mniej niż 8 portów.
- Urządzenie musi mieć możliwość tworzenia zagregowanych linków logicznych, składających się z interfejsów fizycznych wychodzących z różnych przełączników pracujących w stosie.
- 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).
- Przełącznik musi obsługiwać protokół LLDP i LLDP-MED.
- Urządzenie musi obsługiwać routing między sieciami VLAN – routing statyczny, oraz protokół routingu dynamicznego RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 8 000.
- Przełącznik musi posiadać możliwość rozbudowania, poprzez zastosowanie licencji, o funkcjonalność routingu OSPF, BGP oraz PIM a także IGMP v1/v2/v3, Bidirectional Forwarding Detection, 802.1ag oraz 802.1ad (QinQ).
- Urządzenie musi pozwalać na zarządzanie po IPv6.
- 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.
- Urządzenie musi obsługiwać filtrowanie ruchu 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.
- Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping.
- 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.
- 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.
- 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 routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem.
- Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 20 poprzednich, kompletnych konfiguracji.
- Urządzenie musi spełniać standard TL9000.
- Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego przez producentów kanału sprzedaży, na terenie Unii Europejskiej – do oferty należy dołączyć oświadczenie producenta lub autoryzowanego dystrybutora sprzętu i oprogramowania poświadczające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.

Minimalne wymagania techniczne dla: GigabitSwitch 48 portów STACK 10 Gb bez PoE

- Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie rack.

Załącznik nr 1 do Ogłoszenia

- 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. Wymiana modułu uplink nie może wymagać wyłączenia przełącznika. Porty uplink muszą akceptować również wkładki SFP umożliwiając obsługę połączeń uplink Gigabit Ethernet.
- 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. Przełączniki pracujące w stosie, pełniące role control plane, muszą posiadać funkcje synchronizacji stanów protokołów L2 i L3, tablic routingu oraz tablic forwardingu.
- 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).
- Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
- Przełącznik musi być wyposażony w nie mniej niż 1 GB pamięci Flash oraz 1 GB pamięci DRAM.
- Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.
- Przełącznik musi posiadać architekturę non-blocking. Wydajność przełączania w warstwie 2 nie może być niższa niż 175 Gb/s i 130 milionów pakietów na sekundę. Przełącznik nie może obsługiwać mniej niż 16 000 adresów MAC.
- Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
- Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4000. 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.
- Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 32 grupy LAG, po nie mniej niż 8 portów.
- Urządzenie musi mieć możliwość tworzenia zagregowanych linków logicznych, składających się z interfejsów fizycznych wychodzących z różnych przełączników pracujących w stosie.
- 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).
- Przełącznik musi obsługiwać protokół LLDP i LLDP-MED.
- Urządzenie musi obsługiwać routing między sieciami VLAN – routing statyczny, oraz protokół routingu dynamicznego RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 8 000.
- Przełącznik musi posiadać możliwość rozbudowania, poprzez zastosowanie licencji, o funkcjonalność routingu OSPF, BGP oraz PIM a także IGMP v1/v2/v3, Bidirectional Forwarding Detection, 802.1ag oraz 802.1ad (QinQ).
- Urządzenie musi pozwalać na zarządzanie po IPv6.
- 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.
- 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.
- Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping.

Załącznik nr 1 do Ogłoszenia

- 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.
- 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.
- 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 routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem.
- Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 20 poprzednich, kompletnych konfiguracji.
- Urządzenie musi spełniać standard TL9000.
- Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego przez producentów kanału sprzedaży, na terenie Unii Europejskiej – do oferty należy dołączyć oświadczenie producenta lub autoryzowanego dystrybutora sprzętu i oprogramowania poświadczające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.

Minimalne wymagania techniczne dla: GigabitSwitch 48 portów STACK 40 Gb bez PoE

- Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie rack.
- Przełącznik musi posiadać 48 portów dostępowych Ethernet 10/100/1000 Auto-MDI/MDIX oraz 4 wbudowane porty 40 Gigabit Ethernet QSFP+.
- Przełącznik musi posiadać możliwość wyposażenia w dodatkowe 4 porty uplink obsługujące wkładki 1 Gigabit Ethernet oraz 10 Gigabit Ethernet SFP+. Wszystkie porty dostępowe 10/100/1000 oraz 40 Gigabit Ethernet muszą być aktywne po wyposażeniu przełącznika w moduł uplink.
- Przełącznik musi umożliwiać stworzenie stosu (w postaci pętli) liczącego nie mniej niż 10 urządzeń. Do łączenia w stos muszą być zastosowane połączenia o prędkości co najmniej 40 Gb/s. Przełącznik musi pozwalać również na stworzenie stosu przełączników połączonych każdy z każdym (full mesh) dla nie mniej niż 5 urządzeń. Jeśli funkcja stackowania wymaga licencji i/lub dodatkowych modułów, elementy te muszą zostać dostarczone wraz z przełącznikiem.
- 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.
- Przełącznik musi posiadać wymienny zasilacz AC. Przełącznik musi być wyposażony w wewnętrzny redundantny zasilacz. Urządzenie musi posiadać co najmniej 2 moduły wentylacji. Przepływ powietrza przód-tył. Zarówno zasilacz, jak i moduł wentylacji muszą posiadać możliwość wymiany podczas pracy urządzenia (hot swap). Urządzenie musi posiadać panel LCD z przyciskami, pozwalający na wykonywanie podstawowych czynności związanych z zarządzaniem (adresacja IP, reset).
- Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
- Przełącznik musi być wyposażony w nie mniej niż 2 GB pamięci Flash oraz 2 GB pamięci DRAM.
- Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.
- Wydajność przełączania w warstwie 2 nie może być niższa niż 496 Gb/s i 365 milionów pakietów na sekundę. Przełącznik nie może obsługiwać mniej niż 64 000 adresów MAC.
- Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
- Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4000. Przełącznik musi obsługiwać mechanizm Q-in-Q (802.1ad). Urządzenie musi wspierać protokół MVRP.

Załącznik nr 1 do Ogłoszenia

- Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 128 grupy LAG, nie mniej niż 16 portów w grupie.
- Urządzenie musi mieć możliwość tworzenia zagregowanych linków logicznych, składających się z interfejsów fizycznych wychodzących z różnych przełączników pracujących w stosie.
- 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 (nie mniej niż 64 instancje MSTP).
- Przełącznik musi obsługiwać protokół LLDP i LLDP-MED.
- Urządzenie musi obsługiwać routing statyczny oraz protokół RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 16 000 prefiksów.
- Urządzenie musi posiadać możliwość obsługi protokołu VRRP, protokołów routingu dynamicznego OSPFv2/v3 oraz routingu multicast w postaci PIM-SM, PIM-DM, PIM-SSM oraz IGMP.
- Urządzenie musi posiadać możliwość uruchomienia protokołów routingu dynamicznego IS-IS, BGP zarówno dla IPv4 i IPv6.
- Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3. 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 12 kolejek per port fizyczny.
- Urządzenie musi obsługiwać filtrowanie ruchu co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo nie mniej niż 3000 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.
- Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping.
- Przełącznik musi obsługiwać Ethernet Ring Protection Switching.
- 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). Przełącznik musi obsługiwać co najmniej następujące typy EAP: MD5, TLS, TTLS, PEAP.
- Przełącznik musi obsługiwać Private VLANs.
- Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
- 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 routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem.
- Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim.

Załącznik nr 1 do Ogłoszenia

Część 2: Oprogramowanie do monitoringu aktywności użytkowników – 50-150 urządzeń.

Opis ogólny

Kompleksowe, zautomatyzowane, skalowalne oprogramowanie do badania, analizowania i raportowania otoczenia sieciowego ze szczególnym uwzględnieniem:

- monitorowania punktów wejścia/wyjścia danych w postaci nośników USB oraz wydruków
- monitorowania działalności użytkowników na stacjach końcowych z mechanizmami wsparcia
- kontroli licencji i oprogramowania

Dopuszcza się warianty cenowe w zależności od ilości równocześnie monitorowanych urządzeń:

Opcja 1: 50 urządzeń

Opcja 2: 100 urządzeń

Opcja 3: 150 urządzeń

Minimalne wymagania techniczne

Oprogramowanie musi posiadać oficjalne wsparcie producenta. Na żądanie Zamawiającego Wykonawca musi dostarczyć dla celów testowych nośniki oraz bezpłatną licencję czasową (na okres minimum 30 dni) oferowanego oprogramowania oraz zainstalować oferowane oprogramowanie we wskazanym przez Zamawiającego środowisku. Zamawiający przeprowadzi testy zgodności oferowanego oprogramowania z wymogami specyfikacji technicznej. Wszystkie elementy składowe oprogramowania muszą pochodzić od jednego producenta. Oprogramowanie winno zapewniać następujące funkcjonalności:

- **Monitorowanie sieci**
  - Wykrywanie i wizualizacja sieci na modyfikowalnych podkładach graficznych
  - Monitorowanie pracy urządzeń sieciowych (SNMP)
  - Monitoring pracy komputerów z Windows przez WMI
  - Monitoring usług TCP/IP
  - Alarmy – powiadomienia, akcje korekcyjne
  - Monitorowanie aktywności na portach switch'y
  - Obsługa trapów SNMP
  - Monitorowanie stanu usług Windows
  - Wpisy dziennika zdarzeń Windows
- **Sprzęt i oprogramowanie**
  - Wykrywanie konfiguracji sprzętowej
  - Wykrywanie zainstalowanego oprogramowania
  - Numery seryjne oprogramowania Microsoft
  - Historia zmian w konfiguracji
  - Audyt legalności oprogramowania
  - Audyt plików multimedialnych
  - Czytelne zestawienia konfiguracji
  - Dane administracyjne (Środki Trwałe)
- **Aktywność użytkowników**
  - Ogólne informacje o aktywności użytkownika
  - 10 najczęściej oglądanych stron internetowych
  - Monitoring użycia aplikacji
  - Odwiedzane strony WWW (czas i ilość wizyt)
  - Szczegółowy monitoring czasu pracy

- Ruch sieciowy generowany przez użytkownika
- Audyt i koszty wydruków

- **Interaktywny helpdesk**
  - Zarządzanie zgłoszeniami
  - Powiadomienia w czasie rzeczywistym
  - Widok zgłoszenia odświeżany w czasie rzeczywistym
  - Wbudowany zdalny dostęp z możliwym pytaniem użytkownika o zgodę
  - Zintegrowany czat
  - Import użytkowników z Active Directory
  - Komunikaty rozsyłane do użytkowników z możliwością potwierdzenia
  - Automatyzacje bazujące na założeniu: warunek → akcja
  - Baza wiedzy
- **Bezpieczeństwo danych**
  - Lista urządzeń aktualnie podłączonych w sieci
  - Identyfikacja urządzeń po numerach seryjnych
  - Definiowanie praw dostępu do wybranych nośników danych
  - Historia operacji wykonywanych na urządzeniach
  - Uprawnienia dostępu tworzone na poziomie urządzenia i Active Directory
- **Zarządzanie uprawnieniami administratorów**
  - Dostęp do serwera aplikacji z konsoli w sieci lokalnej
  - Podgląd informacji z przeglądarki internetowej
  - Jednoczesna praca wielu administratorów
  - Zróżnicowane uprawnienia dostępu dla różnych użytkowników systemu

Załącznik nr 1 do Ogłoszenia

Część 3: Oprogramowanie do monitoringu sieci – 50-150 stacji roboczych, 10-50 serwerów.

Opis ogólny

Zautomatyzowane, skalowalne oprogramowanie do monitorowania, analizowania logów (dzienników zdarzeń), raportowania kontroli zmian w: Microsoft® Active Directory®, Microsoft® Windows Server®, Microsoft® SQL Server®, Microsoft® Exchange Server®, serwerów plików w całym przedsiębiorstwie wraz z monitorowaniem urządzeń sieciowych.

Dopuszcza się warianty cenowe w zależności od ilości równocześnie monitorowanych urządzeń:

Opcja 1: 50 stacji roboczych, 10 serwerów i urządzeń sieciowych

Opcja 2: 100 stacji roboczych, 30 serwerów i urządzeń sieciowych

Opcja 3: 150 stacji roboczych, 50 serwerów i urządzeń sieciowych

Minimalne wymagania techniczne

Oprogramowanie musi posiadać oficjalne wsparcie producenta. Na żądanie Zamawiającego Wykonawca musi dostarczyć dla celów testowych nośniki oraz bezpłatną licencję czasową (na okres minimum 30 dni) oferowanego oprogramowania oraz zainstalować oferowane oprogramowanie na wskazanym przez Zamawiającego środowisku. Zamawiający przeprowadzi testy zgodności oferowanego oprogramowania z wymogami specyfikacji technicznej. Wszystkie elementy składowe oprogramowania muszą pochodzić od jednego producenta. Oprogramowanie winno zapewniać następujące funkcjonalności:

- **Moduł do raportowania:**
  - Narzędzie nie powinno instalować, żadnego dodatkowego oprogramowania (agentów) na serwerach/komputerach, z których zbiera informacje
  - Narzędzie powinno umożliwiać instalację na następujących systemach: Windows XP/Vista/7/2000/2003/2008/ 2008 R2/2012/2012R2
  - Narzędzie powinno umożliwiać tworzenie raportów online oraz historycznych na temat zmian konfiguracyjnych w środowisku Active Directory/Windows
  - Powinno umożliwiać tworzenie raportów w różnych formatach np. PDF, HTML, CSV, XLS, RTF, TXT.
  - Narzędzie powinno umożliwiać tworzenie raportów z infrastruktury AD/Windows, serwerów plików oraz serwerów MS SQL w trybie offline (komputer z zainstalowanym oprogramowaniem znajduje się poza siecią)
  - Narzędzie powinno posiadać możliwość automatycznego generowania raportów i wysyłania ich do odpowiednich osób w odpowiednim formacie
  - Powinno umożliwiać szybkie tworzenie własnych raportów oraz ich personalizację
  - Powinno zbierać, przechować i raportować informacje na temat użytkowników, grup użytkowników, stacji roboczych/serwerów (sprzęt, oprogramowanie, rejestry, zasoby), Active Directory, uprawnień NFTS do folderów/plików/usług/rejestrów.
  - Powinno umożliwiać tworzenie własnych widoków opartych o zdefiniowane przez użytkownika zbiory zbudowane z obiektów sieciowych, typów obiektów, podsieci IP itp..
  - Powinno umożliwiać wykrywanie luk w bezpieczeństwie za pomocą wbudowanych raportów takich jak np. zagnieżdżenia grup, cyrkulujące grupy, użytkownicy z pustymi hasłami.
  - Powinno prezentować statystyki zmian online (najlepiej w formie wykresów kołowych) w domenie Active Directory/Windows
  - Powinno wspierać systemy Windows XP/Vista/7/2000/2003/2008/2008 R2/2012 R2, z których zbiera informacje,

- Powinno raportować środowisko pod kątem regulacji Compliance (SOX,HIPAA, ISO 17799, COBIT, ITIL) oraz wewnętrznych wymogów audytowych,
- Powinno umożliwiać filtrowanie raportów po dowolnych polach i atrybutach (zakres czasu, użytkownicy, komputery, typ zdarzeń, itp.),
- Powinno umożliwiać tworzenie własnych raportów,
- Powinno umożliwiać tworzenie raportów graficznych,
- Narzędzie powinno przechowywać dane historyczne w bazie MS SQL Server 2005/2008/2008R2/2012/2014 lub Microsoft SQL Express

- **Moduł do monitorowania logów:**
  - Powinno umożliwiać kompresje logów
  - Powinno umożliwiać archiwizację logów w formie natywnej
  - Umożliwiać automatyczne kolekcjonowanie logów oraz ich filtrację, filtrację krytycznych ID, kompresję (40:1), szyfrowanie 3DES (168bit) oraz archiwizację na systemie plików (repozytorium
  - Powinno wykorzystywać bazę danych MS SQL Server do celów raportujących oraz korelacji i powiadamiania na temat incydentów bezpieczeństwa
  - Powinno monitorować krytyczne logi zmian na plikach oraz aktywność użytkowników,
  - Umożliwiać definiowanie własnych użytkowników i grup bezpieczeństwa mających dostęp do narzędzia (definiowane role użytkowników)
  - Instalacja, zarządzanie oraz monitorowanie agentów powinna odbywać się z centralnego miejsca,
  - Oferować możliwość definiowania lub korzystania z wbudowanych logicznych kolekcji komputerów, na których będą zbierane i monitorowane logi,
  - Umożliwiać importowanie historycznych danych logów z repozytorium do bazy MS SQL do celów analitycznych poprzez wykorzystanie gotowych (własnych) polityk importu danych,
  - Monitorować w czasie rzeczywistym krytyczne logi lub nietypowe zdarzenia (kasowanie plików, zmiana uprawnień, itp.),
  - Oferować monitorowanie zdarzeń przy pomocy strony Web oraz konsoli, gdzie można tworzyć różne profile powiadomień oraz przydzielać różne osoby odpowiedzialne za rozwiązywanie problemów z bezpieczeństwem,
  - Oferować powiadamianie oficerów bezpieczeństwa lub administratorów o krytycznych zdarzeniach lub incydentach bezpieczeństwa w postaci: net send, mail,
  - Podejmować automatyczne akcje po wykryciu zdarzenia: uruchomienie skryptu, restart agenta, restart serwera, uruchomienie programu z parametrami, ustanowienie polityki audytu, wysłanie SNMP Trap
  - Integrować się z Microsoft Operations Manager oraz SCOM
  - Raporty mogą być generowane automatycznie zaraz po procesie kolekcjonowania logów, dystrybuowane w przeróżnych formatach(HTML, XML, PDF, CSV oraz TXT czy Excel) i na różne sposoby(e-mail, MS Sharepoint, serwer ftp, Web portal, udział w sieci).
  - Umożliwiać udostępnianie raportów są dostępne poprzez interfejs Web
  - Wykorzystywać wbudowaną funkcjonalności MS SQL Server Reporting Services do generowania i tworzenia raportów,
  - Umożliwiać filtrowanie raportów po dowolnych polach i atrybutach (zakres czasu, użytkownicy, komputery, typ zdarzeń, itp.),
  - Umożliwiać tworzenie własnych raportów,
  - Umożliwiać tworzenie raportów graficznych,

Załącznik nr 1 do Ogłoszenia

Oferować dwupoziomową architekturę składowania logów: Repozytorium – podstawowe miejsce składowania logów (dysk) - mocno skompresowane (40:1), zabezpieczone archiwum logów w formacie natywnym przeznaczone do wydajnego, taniego i długoterminowego przechowywania wszystkich logów ze środowiska sieciowego. Dane z repozytorium mogą być importowane do bazy SQL w dowolnym momencie. Repozytorium zawiera logi w formacie natywnym.

Baza danych SQL – wspierane są wszystkie wersje serwera MS SQL Server. Służy tylko i wyłącznie do celów analityczno-raportujących, gdyż przechowywanie wszystkich logów w bazie jest nieefektywne, kosztowne i zajmuje dużo przestrzeni na dysku.

- Oferować możliwość monitorowania i zbierania logów.
- Narzędzie powinno umożliwiać tworzenie raportów online oraz historycznych na temat zmian konfiguracyjnych w środowisku Active Directory/Windows
- Powinno posiadać predefiniowane polityki audytu zbierające i monitorujące logi na różnych typach serwerów.
- Narzędzie powinno posiadać możliwość automatycznego generowania raportów i wysyłania ich do odpowiednich osób w odpowiednim formacie
- Powinno umożliwiać szybkie tworzenie własnych raportów oraz ich personalizację
- Powinno umożliwiać tworzenie własnych widoków opartych o zdefiniowane przez użytkownika zbiory zbudowane z obiektów sieciowych, typów obiektów, podsieci IP itp..
- Powinno oferować monitorowanie zdarzeń przy pomocy strony Web oraz konsoli, gdzie można tworzyć różne profile powiadomień oraz przydzielać różne osoby odpowiedzialne za rozwiązywanie problemów z bezpieczeństwem,
- Powinno oferować powiadamianie oficerów bezpieczeństwa lub administratorów o krytycznych zdarzeniach lub incydentach bezpieczeństwa w postaci: net send, mail,
- Powinno podejmować automatyczne akcje po wykryciu zdarzenia: uruchomienie skryptu, restart agenta, restart serwera, uruchomienie programu z parametrami, ustanowienie polityki audytu, wysłanie SNMP Trap
- Powinno oferować analizę anomalii bezpieczeństwa, np. logowanie się użytkownika z innego komputera niż zwykle, logowanie się użytkowników poza godzinami pracy
- Powinno dostarczać interfejs do rozwiązywania i opisywania problemów związanych z monitorowanymi zdarzeniami na systemach
- Powinno automatyczne kolekcjonować logi środowiska Active Directory, oraz umożliwiać ich filtrowanie po krytycznych ID oraz kompresowanie
- Powinno kompresować logi podczas przesyłania przez sieć
- Powinno zbierać logi o dowolnych porach dnia
- Powinno zbierać logi przez wolne łącza
- Powinno podejmować akcję po wykryciu incydentu bezpieczeństwa (uruchomienie skryptu, uruchomienie programu, wysłanie maila, wysłanie SNMP Trap).
- Powinno umożliwiać zbieranie i monitorowanie logów na serwerach znajdujących się za firewallem lub poza domeną Active Directory.

Załącznik nr 1 do Ogłoszenia

- **Moduł do audytu serwerów plików:**
  - Rozwiązanie powinno umożliwiać przeprowadzanie inspekcji zmian na folderach, udziałach sieciowych oraz plikach znajdujących się na systemach Windows 2000/2003/2008/2008 R2/2012/2012 R2 bez włączania natywnego audytu Microsoft,
  - Wspierać system plików FAT32 oraz NTFS,
  - Generować w dzienniku zdarzeń Microsoft szczegółowe logi aktywności użytkowników oraz zmian na plikach i folderach,
  - Powinno prezentować statystyki zmian i aktywności online (najlepiej w formie wykresów kołowych) na serwerach plików
  - Powinno na bieżąco pokazywać zmiany na zasobach Serwerów Plików Windows
  - Dostarczać informacje o zmianie na pliku (nazwa, właściciel oraz uprawnienia) takie jak: wartości zmiany atrybutu przed i po zmianie, IP komputera/nazwa komputera, z której została wykonana zmiana, nazwa komputera, na którym zmiana została wykonana, konto użytkownika, z którego została dokonana zmiana, czas wykonania zmiany.
  - Narzędzi powinno umożliwiać opisywanie zdarzeń administracyjnych wykonanych w środowisku Windows File Servers na zasobach dyskowych
  - Narzędzie powinno rejestrować zdarzenia zmian w konfiguracji usług, rejestru systemowego oraz lokalnych użytkowników/grup użytkowników na serwerze Windows
  - Powinno umożliwiać w prosty sposób zapis, import i eksport ustawień audytu na folderach/plikach oraz udziałach sieciowych
  - Narzędzie oferować mechanizm delegowania dostępów do produktu (ról)
  - Umożliwiać w prosty sposób wykluczanie procesów (aplikacji) lub kont użytkowników, których nie chcemy objąć audytem
  - Umożliwiać blokowanie określonego folderu/udziału sieciowego przed niechcianą aktywnością użytkownika
  - Oferować bogate możliwości wykluczania z audytu określonych plików, bądź folderów
  - Rejestrować w logu informacje odczytu, zapisu, przenoszenia, skasowania, zmiany nazwy, utworzenia, zmiany właściciela, zmiany uprawnień do pliku lub folderu na serwerze Windows pokazując jednocześnie wartości zmiany przed i po zmianie, IP komputera oraz konto użytkownika, z którego została dokonana zmiana/dostęp do pliku/folderu,
  - Oferować możliwość blokowania dostępów użytkowników bądź grup do folderów i plików w sytuacji, w której jest potrzeba
  - Powinno pokazywać w logu zmian pełną ścieżkę do pliku, bądź katalogu
  - Umożliwiać definiowanie własnych użytkowników i grup bezpieczeństwa mających dostęp do narzędzia (definiowane role użytkowników)
  - Integrować się z Microsoft Operations Manager oraz SCOM

- **Moduł do audytu MS Active Directory:**
  - Powinno rejestrować zmiany w schemacie Active Directory oraz w konfiguracji kontrolerów domeny,
  - Powinno prezentować statystyki zmian online (najlepiej w formie wykresów kołowych) w domenie Active Directory/Windows
  - Powinno na bieżąco pokazywać zmiany w Active Directory/Windows
  - Powinno generować szczegółowe logi zmian i prób zmian, takich jak nieuprawnione akcje administracyjne na obiektach GPO/ AD

- Narzędzie powinno dostarczać informacje o zmianie obiektu Active Directory takie jak: wartości zmiany przed i po zmianie, IP komputera/nazwa komputera, z której została wykonana zmiana, nazwa komputera, na którym zmiana została wykonana, konto użytkownika, z którego została dokonana zmiana, czas wykonania zmiany.
- Narzędzie powinno umożliwiać opisywanie zdarzeń administracyjnych wykonanych w środowisku Active Directory
- Narzędzie powinno umożliwiać zawnioskowanie o wycofanie zmiany na obiekcie AD z konsoli narzędzia monitorującego
- Narzędzie powinno rejestrować zdarzenia zmian w konfiguracji usług, rejestru systemowego
- Oferować bogate możliwości selekcji atrybutów obiektów Active Directory do audytu
- Powinno monitorować krytyczne logi bezpieczeństwa,
- Powinno umożliwiać definiowanie własnych użytkowników i grup bezpieczeństwa mających dostęp do narzędzia (definiowane role użytkowników)Instalacja, zarządzanie oraz monitorowanie agentów powinna odbywać się z centralnego miejsca,
- Powinno umożliwiać definiowanie lub korzystanie z wbudowanych logicznych kolekcji komputerów, na których będą zbierane i monitorowane logi,
- Powinno umożliwiać importowanie historycznych danych logów z repozytorium do bazy MS SQL do celów analitycznych poprzez wykorzystanie wbudowanego mechanizmu polityk importu danych,
- Powinno monitorować w czasie rzeczywistym (real-time) krytyczne logi lub nietypowe zdarzenia (zachowania użytkowników, logowania, nagminne resetowanie haseł, kilkukrotne nieudane logowania, itp.),
- Powinno posiadać funkcjonalność zabezpieczania krytycznych obiektów w katalogu AD oraz obiektach GPO przed modyfikacją, zmianą, kasowaniem i tworzeniem,
- Powinno umożliwiać generowane automatycznie raportów zaraz po procesie kolekcjonowania logów, dystrybuowane w przeróżnych formatach(HTML, XML, PDF, CSV oraz TXT i Microsoft Word, Visio czy Excel) i ich dystrybucję na różne sposoby(e-mail, serwer ftp, Web portal, udział w sieci).
- Powinno wykorzystywać wbudowaną funkcjonalności MS SQL Server Reporting Services do generowania i tworzenia raportów historycznych,
- Powinno umożliwiać filtrowanie raportów po dowolnych polach i atrybutach (zakres czasu, użytkownicy, komputery, typ zdarzeń, itp.),
- Powinno umożliwiać tworzenie raportów graficznych,
- Powinno zabezpieczać logi przed ich utratą po stronie systemu operacyjnego w szczególności w sytuacjach takich jak wyczyszczenie logów bądź nadpisanie
- Narzędzie powinno mieć możliwość konfigurowania obciążenia procesora maszyny podczas zbierania logów
- Powinno oferować łatwą instalacja agentów poprzez sieć
- Narzędzie powinno umożliwiać wyszukiwania podobne wyszukiwania – wyszukiwanie zdarzeń użytkownika bądź obiektu
- Umożliwiać generowanie kompleksowych raportów wg. najlepszych praktyk i regulacji standardów zgodności dla SOX, PCI-DSS, HIPAA, FISMA, GLBA i wiele innych

Załącznik nr 1 do Ogłoszenia

- **Moduł do monitorowania urządzeń sieciowych:**
  - Oprogramowanie dostarcza łatwo konfigurowalny interfejs metodą „przeciągnij i upuść" (ang. drag and drop).
  - Oprogramowanie umożliwia dostęp do interfejsu użytkownika za pomocą przeglądarki internetowej.
  - Oprogramowanie umożliwia bezagentowe monitorowanie z wykorzystaniem protokołach SNMP i WMI.
  - Oprogramowanie umożliwia konfiguracje systemu powiadomień za pomocą SMS lub email.
  - Oprogramowanie pozwala na eskalację powiadomień jeżeli wykryte zdarzenie nie zostanie rozwiązane w zdefinowanym przez administratora czasie.
  - Oprogramowanie umożliwia prowadzenie ewidencji środków trwały dla wszystkich monitorowanych urządzeń.
  - Oprogramowanie umożliwia tworzenie raportów z podziałem na użytkowników, działy, grupy oraz całego przedsiębiorstwa.

Załącznik nr 1 do Ogłoszenia

Część 4: Oprogramowanie do kontroli i autoryzacji dostępu urządzeń – 150 urządzeń.

Opis ogólny

Kompleksowe, zautomatyzowane oprogramowanie do monitorowania, kontroli i autoryzacji dostępu wszystkich urządzeń, w tym mobilnych podłączanej do sieci wewnętrznej.

Ilość równocześnie monitorowanych urządzeń co najmniej 150 szt.

Minimalne wymagania techniczne

Oprogramowanie musi posiadać oficjalne wsparcie producenta. Na żądanie Zamawiającego Wykonawca musi dostarczyć dla celów testowych nośniki oraz bezpłatną licencję czasową (na okres minimum 30 dni) oferowanego oprogramowania oraz zainstalować oferowane oprogramowanie we wskazanym przez Zamawiającego środowisku. Zamawiający przeprowadzi testy zgodności oferowanego oprogramowania z wymogami specyfikacji technicznej. Wszystkie elementy składowe oprogramowania muszą pochodzić od jednego producenta. Oprogramowanie winno zapewniać następujące funkcjonalności:

- System musi być dostarczany w postaci maszyn wirtualnych w formacie OVF (zgodnych z VmWare ESXi serwer wersja 6.0)
- System musi posiadać wbudowany portal uwierzytelniający
  - Portal musi się automatycznie dostosowywać formatem do podłączonego urządzenia (komputer, tablet, telefon)
  - Musi istnieć możliwość stworzenia własnej wersji portalu przez administratora
- W system musi być wbudowany serwer RADIUS
  - Musi istnieć możliwość zarządzania atrybutami zwracanymi przez serwer RADIUS
- Informacje o kontach użytkowników muszą być przechowywane w relacyjnej bazie danych
- System musi umożliwiać bezpośrednią integrację z LDAP oraz Active Directory
- System musi umożliwiać automatyczną autoryzację urządzeń i użytkowników domenowych
- System musi umożliwiać zwracanie zadeklarowanych atrybutów RADIUS w zależności od tego czy użytkownik wykorzystuje komputer domenowy
- System musi umożliwiać zwracanie zadeklarowanych atrybutów RADIUS w zależności od tego czy użytkownik wykorzystuje urządzenia spoza domeny Active Directory
- Zarządzanie funkcjami systemu musi odbywać się przez przeglądarkę z kryptograficznym zabezpieczeniem transmisji (SSL/HTTPS)
- System musi zapewniać tworzenie uprzywilejowanych użytkowników, z uprawnieniami do zarządzania kontami gości (tworzenie kont, masowe tworzenie kont, modyfikacja, kasowanie)
- System musu posiadać wbudowany portal do samodzielnej rejestracji kont przez użytkowników-gości
- Musi istnieć możliwość dostarczania informacji o rejestracji konta gościnnego przez SMS z wykorzystaniem zewnętrznych dostawców usług SMS – usługa musi być dostępna do natychmiastowej integracji z przynajmniej 3 dostawcami usług (po wykupieniu abonamentu u danego dostawcy)
- System musi posiadać portal do automatycznej rejestracji urządzeń mobilnych oraz komputerów spoza domeny Active Directory (BYOD - Bring Your Own Device), obsługujący nie mniej niż następujące systemy operacyjne – Apple iOS oraz MAC OSX, Android, Windows XP/7/8/10
- System musi posiadać mechanizm zarządzania uprawnieniami użytkowników, którzy będą mogli rejestrować swoje urządzenia
- System musi posiadać wbudowane mechanizmy wydawania i zarządzania certyfikatami cyfrowymi
- System musi posiadać wbudowane narzędzie do profilowania sieci poprzez zbieranie informacji o końcówkach za pomocą DHCP oraz SNMP
- System musi posiadać wbudowany skaner sieciowy umożliwiający przynajmniej weryfikowanie otwartych portów na końcówce

Załącznik nr 1 do Ogłoszenia

- Musi być dostępne API XML/RPC
- Muszą być dostępne narzędzia diagnostyczne do weryfikacji połączeń między systemami
- System musi zapewniać generowanie raportów dotyczących ilości użytkowników oraz trendów
- System musi obsługiwać nie mniej niż 500 unikalnych punktów końcowych (endpoints)
- System musi zbyć dostarczony z licencjami obsługującymi do 25 agentów umożliwiających ocenianie bezpieczeństwa punktu końcowego (endpoints)
- Wraz z systemem musi zostać dostarczone wsparcie techniczne na okres 2 lat.