Załącznik nr 3 do SWZ

**Szczegółowy opis przedmiotu zamówienia do postępowania o udzielenie zamówienia na dostawę, wdrożenie oraz utrzymanie zintegrowanego systemu bezpieczeństwa informacji i infrastruktury IT oraz agregatów prądotwórczych dla Urzędu Gminy Czudec oraz niektórych jednostek organizacyjnych Gminy,**

**finansowanego z Programu Fundusze Europejskie na Rozwój Cyfrowy (FERC)**

**Priorytet II Zaawansowane usługi cyfrowe**

**Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa**

**Fundusz Europejski Fundusz Rozwoju Regionalnego (EFRR)**

**Numer naboru FERC.02.02-CS.01-001/23**

**CZĘŚĆ DEDYKOWANA DLA ZADANIA NR 1: Dostawa zintegrowanego systemu bezpieczeństwa informacji i infrastruktury IT na potrzeby funkcjonowania Urzędu Gminy w Czudcu i wybranych jednostek organizacyjnych gminy.**

**I. Uwagi ogólne:**

Niniejszy dokument prócz zdefiniowania minimalnych wymagań dotyczących przedmiotu zamówienia, będzie również pełnił funkcje przedmiotowego środka dowodowego w rozumieniu ustawy Prawo zamówień publicznych z dnia 11.09.2019 r. (tekst jednolity Dz. U. z 2023 r. poz. 1605 z późniejszymi zmianami). W związku z powyższym Wykonawca zobowiązany jest do dokonania szczegółowej analizy załącznika pod kątem sformułowanych wymogów i wypełnienie stosownych kolumn tabel ujętych w części II i III załącznika (wymóg nie dotyczy: cz. 23 Usługa instalacji i konfiguracji środowiska sieciowego, tu Wykonawca zobowiązany jest jedynie potwierdzić realizację przedmiotowego zakresu w ramach złażonej oferty w cz. II i III załącznika wybierając odpowiednią opcję). Następnie Wykonawca zobowiązany jest do dołączenia wypełnionego dokumentu do złożonej oferty.

W części II Wykonawca zobowiązany jest do podania oferowanego modelu lub wersji oraz producenta oferowanego asortymentu (w kolumnie 3).

W części III natomiast Wykonawca zobowiązany jest do odniesienia się do opisanego wymogu i wpisanie danych (w kolumnie 3), które będą miały za zadanie jednoznaczne potwierdzenie spełnienie danego wymogu. Wpisy ogólne typu: „zgodne z SWZ” nie będą traktowane przez Zamawiającego jako prawidłowe.

Zamówione urządzenia i oprogramowanie, mają być fabrycznie nowe, kompletne, nieużywane i pozbawione wad fizycznych i prawnych. Zamawiający wyklucza dostawę sprzętu używanego, poleasingowego, powystawowego, po zwrocie itp. Nie dopuszcza się zaoferowania sprzętu refurbished. Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający. Zamawiający nie dopuszcza stosowania licencji używanej, przeniesionej z innego sprzętu oraz licencji typu refurbished. Nie dopuszcza się stosowania adapterów, przejściówek, ani innych urządzeń zewnętrznych w celu osiągnięcia wymaganych portów i funkcjonalności urządzeń. Wyjątek stanowi sytuacja, że dopuszczenie adapterów jest wyraźnie opisane w opisie pozycji przedmiotu zamówienia.

Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu   
w odniesieniu do produktów podwójnego zastosowania.

**II. Zestawienie Oferowanego sprzętu, oprogramowania lub usług:**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Przedmiot zamówienia** | **Producent/ Model/Wersja** |
| *1* | *2* | *3* |
| **1.** | **System monitorowania sieci i użytkowników 35 USER** |  |
| **2.** | **Serwer 1 szt.** |  |
| **3.** | **UPS 1 szt.** |  |
| **4.** | **System antywirusowy 35 USER licencja** |  |
| **5.** | **Serwer NAS 1 szt.** |  |
| **6.** | **UPS 1 szt.** |  |
| **7.** | **Urządzenie UTM 1 szt.** |  |
| **8.** | **Przełącznik sieciowy 1 szt.** |  |
| **9.** | **Serwer z systemem operacyjnym dla GOPS w Czudcu 1 szt.** |  |
| **10.** | **Zasilacze awaryjne UPS do stanowisk komputerowych dla GOPS w Czudcu 10 szt.** |  |
| **11.** | **Serwer NAS dla GOPS w Czudcu 1 szt.** |  |
| **12.** | **UTM wraz ze wsparciem technicznym oraz subskrypcjami dla GOPS w Czudcu 1 szt.** |  |
| **13.** | **Serwer z systemem operacyjnym dla ZEAS w Czudcu 1 szt.** |  |
| **14.** | **Zasilacze awaryjne UPS do stanowisk komputerowych dla ZEAS w Czudcu 10 szt.** |  |
| **15.** | **Zarządzany przełącznik sieciowy dla ZEAS w Czudcu 1 szt.** |  |
| **16.** | **Serwer NAS dla ZEAS w Czudcu 1 szt.** |  |
| **17.** | **UTM wraz ze wsparciem technicznym oraz subskrypcjami dla ZEAS w Czudcu 1 szt.** |  |
| **18.** | **Zasilacze awaryjne UPS do stanowisk komputerowych dla ZWK w Czudcu 9 szt.** |  |
| **19.** | **Zarządzany przełącznik sieciowy dla ZWK w Czudcu 1 szt.** |  |
| **20.** | **Serwer NAS dla ZWK w Czudcu 1 szt.** |  |
| **21.** | **UTM wraz ze wsparciem technicznym oraz subskrypcjami dla ZWK w Czudcu 1 szt** |  |
| **22.** | **Serwer z systemem operacyjnym dla ZWK w Czudcu 1 szt.** |  |
| **23.** | **Zakup usługi konfiguracyjnej pozwalającej wdrożyć nowe rozwiązania informatyczne.** | **TAK/NIE\*** |

*\*Wybrać odpowiednie.*

**III. PARAMETRY SPRZĘTU I OPROGRAMOWANIA**

1. **System monitorowania sieci i użytkowników (SIEM) 35 USER**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **LICENCJA** | W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją bezterminową.  Oprogramowanie musi posiadać wsparcie min. do dnia 25-05-2026 roku, w ramach wsparcia, Zamawiający musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji oprogramowania, zgłaszać błędy w Oprogramowaniu do serwisu producenta.  Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.  Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych |  |
| **WYMAGANIA DOT. SYSTEMU BEZPIECZEŃSTWA** | Automatyczne Odkrywanie: Centralny System Bezpieczeństwa (dalej CSB) musi używać różnych metod, takich jak skanowanie sieci, obsługa protokołów SNMP, IPMI, i JMX, aby automatycznie wykrywać i konfigurować urządzenia w sieci.  Monitorowanie Wysokiej Wydajności: CSB musi umożliwiać monitorowanie wydajności przy wykorzystaniu rozwiązań agentowych lub bez agentowych metodami monitorowania (np. przez SNMP, ICMP, IPMI), CSB musi efektywnie zbierać dane o wydajności i dostępności urządzeń. System powinien być skalowalny i umożliwiać obsługę co najmniej 100 urządzeń i metryk.  Elastyczne Wyzwalacze: Wyzwalacze (akcje) w CSB powinny być wyrażeniami logicznymi, które określają warunki dla powiadomień alarmowych. W systemie musi być możliwość definiowania złożonych warunków dla generowania alertów, na przykład po przekroczeniu pewnych progów lub w przypadku wystąpienia określonych wzorców.  Wizualizacja Danych: CSB powinien posiadać intuicyjny i przejrzysty interface, umożliwiający wizualizację danych pod kontem ich analizy. System musi umożliwiać wizualizację przy wykorzystaniu m.in interaktywnych wykresów i grafik ponadto system musi posiadać wbudowaną zaawansowaną wyszukiwarkę umożliwiającą odfiltrowywanie danych i ich wizualizację wg. wybranych kategorii (np. poziom istotności).    Alerty i Powiadomienia: CSB powinien umożliwiać konfigurację zaawansowanych scenariuszy powiadomień, które mogą być wysyłane poprzez e-mail, SMS, czy integracje z systemami biletowymi. Użytkownicy powinni mieć możliwość ustawiania różnych poziomów priorytetów dla alertów, a także definiowania eskalacji dla poważniejszych problemów.  Raportowanie: CSB powinien umożliwiać użytkownikom generowanie szczegółowych raportów dotyczących wydajności i dostępności monitorowanych systemów.  Wsparcie dla Szyfrowania: CSB musi być systemem bezpiecznym, umożliwiającym szyfrowaną komunikację między agentami a serwerem, co zapewnia bezpieczeństwo danych monitorowania.  Skalowalność: Architektura CSB powinna być zaprojektowana z myślą o skalowalności, co powinno pozwalać na łatwą adaptację do rosnących wymagań w miarę rozwoju infrastruktury IT.  Przetwarzanie i Wyszukiwanie Danych: CSB pod kątem agregacji logów musi być oparty na technologii, która umożliwia indeksowanie, wyszukiwanie i analizowanie dużych ilości danych w czasie rzeczywistym. Użytkownicy powinni móc wykonywać skomplikowane zapytania, aby szybko odnaleźć konkretne informacje.  Szybkość i Wydajność: Zaprojektowany do szybkiego przetwarzania dużych ilości danych, co jest kluczowe w środowiskach produkcyjnych z intensywnym ruchem danych.  Elastyczne Zbieranie Danych: CSB musi gromadzić dane z różnych źródeł jednocześnie (co najmniej urządzenia sieciowe, serwery, urządzenia klienckie).  Przetwarzanie i Wzbogacanie Danych: CSB musi posiadać bogaty zestaw filtrów do przetwarzania danych.  Odkrywanie i Analiza Danych: System musi umożliwia użytkownikom przeszukiwanie, przeglądanie i analizowanie zgromadzonych danych ułatwiając identyfikację wzorców i trendów.  Wsparcie dla Wielu Platform: CSB musi być kompatybilny z wieloma systemami operacyjnymi, co najmniej Linux, Windows, macOS.  Treści pojawiające się w interfejsie użytkowników CSB będą spełniać standardy WCAG 2.1 na poziomie AA.  Cały interfejs użytkownika powinien być́ dostosowany pod aktualne wymagania prawne związane z dostępnością̨ serwisów użyteczności publicznej dla osób z niepełnosprawnościami.  Na podstawie uzyskanych efektów serwis będzie mógł być́ udostępniony publicznie.  Treści multimedialne muszą być́ dostępne z poziomu klawiatury i oprogramowania dla osób niepełnosprawnych. Multimedia, które nie mogą̨ być́ z przyczyn technicznych tak zbudowane, by uczynić́ je dostępnymi dla wszystkich użytkowników muszą posiadać́ alternatywny opis tekstowy, który wyjaśnia ich cel i funkcje zastosowania na stronie.  Zgodność́ ze standardami HTML i CSS całego serwisu www.  Kontrast kolorystyczny między tłem, a tekstem musi być́ zgodny z zaleceniami WCAG 2.1 AA.  System CSB musi rejestrować zdarzenia akcje i reakcje użytkowników w CSB. Historia akcji poszczególnych użytkowników musi być raportowana i możliwa do odtworzenia w logach systemowych – chronologicznie. |  |
| **OGÓLE WYMOGI BUDOWY SYSTEMU** | **System musi posiadać budowę modułową, która będzie umożliwiać dodawanie nowych modułów oraz wyłączanie już uruchomionych. Dostarczony i uruchomiony system będzie posiadał co najmniej moduły** |  |
| **MODUŁ ANALIZY PODATNOŚCI** | 1.1. Integracja ze stale aktualizowaną bazą danych CVE (Common Vulnerabilities and Exposures), gromadzącą informację na temat podatności urządzeń i oprogramowania.  System musi być zintegrowany z publicznym i stale aktualizowanym rejestrem gromadzącym i udostępniającym informację na temat znanych podatności w urządzeniach obsługiwanych przez system oraz oprogramowaniu zainstalowanym na urządzeniach Zamawiającego (np. UTM). Połączenie z bazą danych CVE odbywać się ma przy wykorzystaniu udostępnionego API i nie powinno wymagać od użytkowników końcowych konfiguracji.  Synchronizacja z bazą CVE oraz sprawdzenie dodania do niej nowych podatności dotyczących sprzętu i oprogramowania zainstalowanego w infrastrukturze sieciowej jednostki musi odbywać się przynajmniej raz dziennie. Po zalogowaniu do CSB i wybraniu modułu analizy podatności powinny być wyświetlane wszystkie zsynchronizowane informacje wraz z danymi historycznymi. Podatności “nowe”, których użytkownik wcześniej nie widział powinny być w systemie oznaczone np. poprzez pogrubioną czcionkę lub inny kolor.  1.2.  Automatyczne sprawdzenie możliwości występowania podatności w infrastrukturze sieciowej na podstawie zinwentaryzowanych urządzeń i oprogramowania.  System musi automatycznie sprawdzać możliwość wystąpienia nowej podatności tylko na urządzeniach i oprogramowaniu znajdującym się w infrastrukturze sieciowej jednostki, a dokładniej wyszczególnionych (dodanych) w module inwentaryzacji.  1.3.  Powiadamianie użytkownika o nowych podatnościach występujących w jego środowisku IT.  System musi informować użytkownika/administratora o nowych podatnościach występujących w infrastrukturze sieciowej jednostki. System powinien posiadać możliwość włączenia powiadomień na przeglądarkę internetową oraz wskazany przez użytkownika/administratora adres e-mail. Ponadto użytkownik po zalogowaniu się do systemu i wybraniu modułu analizy podatności musi być powiadomiony przez system o występujących nowych podatnościach na poszczególnych hostach infrastruktury sieciowej poprzez np. graficzne wyróżnienie hosta i oprogramowania na nim zainstalowanego. System musi informować użytkownika o treści podatności oraz jej sklasyfikowania (np. podatność krytyczna). |  |
| **MODUŁ MONITORINGU ZASOBÓW** | 2.1.  Monitorowanie zasobów hostów na podstawie zinwentaryzowanych w systemie urządzeń (monitoring obciążenia dysków, procesorów, ruchu sieciowego itp.)  System musi posiadać możliwość monitorowania zasobów wszystkich hostów dodanych w module inwentaryzacji. Monitorowanie, zbieranie informacji na temat obciążenia wybranego hosta musi odbywać się w sposób ciągły w ustalonych krótkich (co najmniej minutowych) odstępach czasowych. Użytkownik po zalogowaniu się do systemu i wybraniu modułu inwentaryzacji musi mieć możliwość wyświetlenia w formie graficznej (wykresów), przebiegów czasowych istotnych parametrów hosta, co najmniej takich jak: obciążenie procesora, obciążenie pamięci, obciążenie dysków, obciążenie ruchu sieciowego, skoki na procesorze, czas oczekiwania na dysk i odczyt i zapis na dysku. Ponadto system musi na bieżąco informować o aktualnym statusie hosta (dostępny, niedostępny).  2.2.  Grupowanie hostów i korelacja obciążeń zasobów pomiędzy hostami  System musi mieć możliwość wyświetlania zgrupowanych wykresów hostów należących do tej samej grupy. Hosty muszą być pogrupowane w zasugerowany przez administratora sieci sposób w celu skorelowania ze sobą istotnych parametrów zasobów, co umożliwi porównanie zachowań poszczególnych hostów na tle grupy. Hosty powinny być podzielone co najmniej, na urządzenia sieciowe (np. serwery) oraz urządzenia końcowe (np. komputery pracowników). Użytkownik musi mieć możliwość filtrowania wykresów na poziomie poszczególnych hostów, oraz tworzenia w systemie nowych grup i wykresów parametrów dostępnych z wybieralnej listy.  2.3.  Wysyłanie alertów i powiadomień dotyczących problemów i zdarzeń występujących na hostach  System musi posiadać funkcjonalność umożliwiającą użytkownikowi/administratorowi skonfigurowanie wysyłania alertów i powiadomień dotyczących problemów i zdarzeń. W systemie musi być możliwość ustawienia wysyłania wiadomości i powiadomień, poprzez wysyłanie komunikatów na przeglądarkę internetową, wysyłanie wiadomości e-mali lub wiadomości sms (w systemie powinna być możliwość dodania bramki sms - Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms). Wysyłane przez system wiadomości muszą zawierać co najmniej informacje na temat występującego zdarzenia/problemu tj. opis, sklasyfikowanie (np. błąd, ostrzeżenie, informacja), data i godzina. Użytkownik/Administrator powinien mieć możliwość ustawienia odbiorcy wiadomości poprzez podanie adresu e-mail, czy w przypadku wiadomości SMS numeru telefonu. Użytkownik musi mieć możliwość wyboru w systemie, przy jakiego typu zdarzeniach i problemach będzie wysyłana wiadomość.  2.4. Funkcja korelacji występujących problemów na hostach z modułem analizy logów    Moduł monitoringu zasobów oprócz przebiegów czasowych parametrów hostów powinien również zawierać informację na temat występujących problemów i zdarzeń na poszczególnych hostach. Użytkownik/Administrator po zalogowaniu się do systemu, wybraniu Modułu Monitoringu zasobów i wyborze konkretnego hosta musi posiadać możliwość prześledzenia zdarzeń i problemów naniesionych na osi czasu. Na osi czasu powinny być wyświetlane tylko “nowe” problemy i zdarzenia oraz te, których status nie został zmieniony na “rozwiązany” bądź “anulowany”. Użytkownik/Administrator musi mieć możliwość zmiany statusu wybranego zdarzenia czy problemu wraz z dodaniem krótkiego opisu w jaki sposób problem został rozwiązany. Użytkownik/Administrator musi mieć możliwość stłumienia często powielającego się problemu, którego jest świadomy i musi poczekać na jego rozwiązanie (po włączeniu opcji tłumienia problemu, system przez pewien czas nie będzie o nim informował/alertował). Wszystkie problemy i zdarzenia raportowane w systemie muszą być skorelowane z logami pochodzącymi z konkretnych hostów. Użytkownik/Administrator po wybraniu w systemie konkretnego problemu występującego na konkretnym hoście po wybraniu zakładki logi musi zostać przekierowany do modułu analizy logów, w którym automatycznie wyświetlone będą tylko logi dotyczące hosta na którym wystąpił problem. Ponadto użytkownik/administrator w ramach tego modułu powinien mieć możliwość zgłoszenia wystąpienia konkretnego problemu do np. zewnętrznego wsparcia IT. W systemie powinna być możliwość integracji systemu z zewnętrznym systemem typu: “help-desk”, przynajmniej poprzez podanie adresu e-mail, na który zostanie wysłane zgłoszenie.  2.5. Kategoryzacja istotności zdarzeń występujących w infrastrukturze sieciowej  Wszystkie zdarzenia i problemy raportowane w systemie muszą być skategoryzowane według ich poziomu istotności (priorytetów). W systemie powinny być identyfikowane problemy z priorytetami w co najmniej 4 stopniowej skali, np: Krytyczny, Wysoki, Średni, Niski. Ponadto, system powinien zapewniać dodatkowe dwa priorytety - zdarzenia nie istotne powinny być również sklasyfikowane w systemie jako informacja, a zdarzenia trudne do sklasyfikowania powinny posiadać priorytet o wartości (niesklasyfikowany).  2.6 Lista predefiniowanych zdarzeń najczęściej występujących w środowiskach IT  System musi być wyposażony w listę wcześniej zdefiniowanych zdarzeń/scenariuszy, które najczęściej występują w środowiskach IT. Użytkownik/Administrator powinien mieć możliwość wybrania konkretnego hosta lub grupy hostów i przypisania im predefiniowanych zdarzeń (np. brak miejsca na dyskach, czy zbyt wysoki ruch sieciowy). W predefiniowanych zdarzeniach/scenariuszach użytkownik/administrator powinien mieć możliwość ustawienia/edycji reguł oraz zmiany wykonywanych operacji, gdy warunki reguł zostaną spełnione. Użytkownik powinien mieć możliwość używania w regułach operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: “==”, “<=”, “>=”, “!=”. Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.  2.7 Dobór oraz dodawanie zdarzeń do konkretnego środowiska IT  System musi umożliwiać użytkownikowi/administratorowi dodawanie własnych zdarzeń/scenariuszy dostosowanych do jego konkretnych potrzeb. Tworzenie nowego zdarzenia w systemie powinno się odbywać poprzez podanie jego unikalnej nazwy, wybranie hosta lub grupy hostów, których dotyczy tworzone zdarzenie, zdefiniowanie warunków opisujących zdarzenie, oraz podanie operacji jakie mają być wykonane, gdy warunki zostaną spełnione. Warunki powinny korzystać z operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: “==”, “<=”, “>=”, “!=”. Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.  2.8 Zdalny dostęp do urządzeń końcowych  System musi umożliwiać zdalne połączenie się do wybranego hosta/urządzenia, które zostało wcześniej odpowiednio skonfigurowane. Zdalny dostęp musi odbywać się poprzez przeglądarkę internetową bez konieczności instalowania dodatkowego oprogramowania. Połączenie zdalne musi być możliwe przy wykorzystaniu co najmniej dwóch protokołów, konkretnie RDP i SSH.  2.9 Wywoływanie predefiniowanych skryptów na urządzeniach końcowych  System musi dawać możliwość wywołania podstawowych skryptów na hostach końcowych, na których został zainstalowany jego agent. Predefiniowane w systemie skrypty muszą obejmować co najmniej: wyłączenie i restart hosta, wysłanie wiadomości tekstowej do hosta, włączenie i wyłączenie blokady ruchu sieciowego, włączenie i wyłączenie trybu izolacji z infrastruktury sieciowej hosta z możliwością zdalnego połączenia się z nim.    2.10 Analiza ruchu sieciowego  System musi posiadać możliwość śledzenia logów pochodzących z urządzeń sieciowych typu UTM zwłaszcza tych najczęściej używanych i polecanych w środowiskach informatycznych. Użytkownik systemu/administrator musi mieć możliwość filtrowania wyświetlanych informacji, co najmniej poprzez podanie przedziału czasowego i wyboru nazwy zinwentaryzowanego urządzenia typu UTM.    2.11 Monitorowanie problemów i zdarzeń występujących na drukarkach  System musi umożliwiać monitorowanie problemów występujących na drukarkach sieciowych wykorzystujących protokół SNMP. System powinien zbierać informacje na temat występujących problemów w osi czasu, umożliwiać tłumienie problemów, wskazywać ich istotność. Ponadto w systemie powinny znajdować się możliwe do pobrania wartości parametrów drukarki oraz informacji na temat dostępności urządzenia. |  |
| **MODUŁ ANALIZY LOGÓW** | 3.1. Przegląd i analiza logów pochodzących z inwentaryzowanych urządzeń/maszyn.  Moduł Analizy Logów i Moduł Monitoringu Zasobów musi być powiązany z Modułem Inwentaryzacji i wykorzystywać informację przez niego posiadane. Użytkownik/Administrator systemu musi posiadać możliwość przeglądania i analizowania logów pochodzących z wszystkich hostów dodanych w Module inwentaryzacji. W ramach modułu system musi agregować logi pochodzące z systemów operacyjnych, aplikacji i systemów dziedzinowych. Agregacja logów powinna odbywać się w sposób ciągły i po osiągnięciu limitu związanego z zasobami dyskowymi serwera nadpisywać historyczne logi, począwszy od najstarszych.  3.2. Możliwość analizy tzw. „customowych” logów pochodzących z dowolnego oprogramowania, w tym systemów dziedzinowych.  System musi posiadać możliwość analizy logów pochodzących z dowolnego oprogramowania, a przede wszystkim z oprogramowania dziedzinowego stosowanego przez Zamawiającego. Użytkownik/Administrator musi mieć możliwość dodawania w module nazwy, lokalizacji i typu tzw. “customowych” logów, które będą agregowane w systemie, w celu późniejszej ich analizy. Zdefiniowane przez Użytkownika/Administratora logi powinny być skorelowane z problemami występującymi na hostach w module monitoringu zasobów. Jeśli wystąpi jakiś problem związany z działaniem np. systemu dziedzinowego, to użytkownik/administrator analizując problemy musi mieć opcję automatycznego przekierowania do logów związanych z tym system.  3.3.  Zawansowane filtrowanie, zarówno po hostach jak i zainstalowanym na nich oprogramowaniu.  Moduł analizy logów musi być wyposażony w zaawanasowaną wyszukiwarkę umożliwiającą użytkownikowi/administratorowi wyszukiwanie i filtrowanie konkretnych logów. System powinien umożliwiać odfiltrowanie logów dla konkretnego hosta, grupy hostów, oprogramowania (w szczególności oprogramowania dziedzinowego - “customlogów”), kategorii, dowolnie wpisanej frazy oraz zakresu czasu (data – godzina, od -do). W Systemie muszą być zastosowane mechanizmy stronicowania, umożliwiające płynne przeglądanie dużej ilości informacji.  3.4. Przegląd i analiza logów dotyczących działań użytkowników.  W module analizy logów muszą być agregowane logi dotyczące działań użytkowników. W zależności od rodzaju systemu czy oprogramowania zainstalowanego na hoście w logach znajdują się informacje dotyczące różnej aktywności użytkowników (m.in. data zalogowania się użytkownika do systemu, data wylogowania, czy wybór konkretnej funkcjonalności). Użytkownik/Administrator CSB musi mieć możliwość sprawdzenia tych aktywności poprze wyszukanie i odfiltrowanie logów po nazwie użytkownika, typie aktywności, czy dowolnie wpisanej frazie.  3.6. Dostęp do logów historycznych.  System oprócz dostępu do aktualnych logów musi uwzględniać również logi historyczne. Użytkownik/Administrator musi mieć możliwość przeglądania wszystkich logów agregowanych na zasobach dyskowych. Ilość oraz zakres czasowy agregowanych logów limitowany ma być tylko zarezerwowaną przestrzenią dyskową na serwerze. Po osiągnięciu założonego limitu, system powinien nadpisywać logi począwszy od najstarszych. Użytkownik/Administrator podobnie jak w przypadku logów aktualnych musi mieć możliwość przeszukiwania oraz filtrowania logów historycznych po hostach, oprogramowaniu, czasie i dowolnie wpisanej frazie.  3.7. Informowanie i powiadomienia dotyczące pojawienia się nowych istotnych logów w obrębie całej infrastruktury sieciowej.  System musi być wyposażony w mechanizmy powiadamiające użytkownika/administratora o pojawieniu się istotnych logów pochodzących z urządzeń infrastruktury sieciowej. System musi posiadać możliwość konfiguracji tych powiadomień pod katem istotności pojawiającego się wpisu w lagach oraz wyboru typu logu (m.in. log systemowy, log “customowy”). Ponadto CSB musi informować użytkownika/administratora o “nowych” zagregowanych logach z poszczególnego hosta. Informacja ta powinna być wyświetlana w systemie po zalogowaniu użytkownika/administratora, a “nowe” logi to logi dodane do systemu od czasu ostatniego logowania użytkownika/administratora.  3.8. Kategoryzacja istotności logów (np.: informacja, ostrzeżenie, błąd).  System musi być wyposażony w mechanizmy kategoryzujące logi pod kontem ich istotności. System w szczególności powinien informować użytkownika/administratora o pojawieniu się logów dotyczących nieprawidłowości działania poszczególnych hostów, czy oprogramowania na nich zainstalowanych. Następnie w zależności od potrzeb użytkownika/administratora system powinien informować o pojawieniu się ostrzeżeń w oprogramowaniu kluczowym dla użytkownika. Jeśli log dotyczy tylko informacji takiej jak zalogowanie się, czy wyłączenie hosta, to użytkownik/administrator nie powinien otrzymywać powiadomienia (alertu), z wyjątkiem logów które użytkownik/administrator uzna za istotne (pomimo tego, że są skategoryzowane jako informacja). |  |
| **MODUŁ EDR/XDR** | 4.1 System musi posiadać własny moduł EDR/XDR, czyli zintegrowane rozwiązanie bezpieczeństwa, którego główne funkcje to: monitorowanie i gromadzenie danych o aktywnościach użytkowników i oprogramowania na urządzeniach końcowych, analiza tych danych w celu identyfikacji wzorców zagrożeń, automatyczne reagowanie na zidentyfikowane zagrożenia w celu ich usunięcia lub powstrzymania, powiadamianie personelu bezpieczeństwa o zidentyfikowanych anomaliach.    4.2 Moduł posiadać podgląd informacji, alertów i zdarzeń występujących w środowisku IT. W CSB powinna być możliwość podglądnięcia statystyk incydentów/zdarzeń oraz ich kategorie. Użytkownik/Administrator z poziomu CSB powinien mieć możliwość uzyskania takich informacji jak rodzaj, nazwa lub źródło incydentu, opis, data wykrycia oraz kategoria/priorytet.    4.3 Oprócz posiadanego modułu EDR/XDR, system musi być otwarty tj. posiadać możliwość integracji z rozwiązaniami EDR/XDR innych producentów (co najmniej ESET, WithSecure, Bitdefender). System musi umożliwiać bezpośrednie przekierowanie do zaawansowanych opcji zintegrowanego systemu EDR/XDR (panelu administracyjnego). Dzięki integracji w module musi znajdować się funkcjonalność umożliwiająca użytkownikowi/administratorowi przejście do panelu administracyjnego systemu EDR/XDR udostępniającego zaawansowane opcje. |  |
| **MODUŁ INWENTARYZACJI** | 5.1 Automatyczny (przy wykorzystaniu agentów), półautomatyczny (przy wykorzystaniu pliku CSV) lub ręczny sposób dodawania hostów oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.  System musi dawać użytkownikowi/administratorowi możliwość dodawania hostów/urządzeń/oprogramowania należących do infrastruktury sieciowej na trzy różne sposoby. Pierwszy dotyczy automatycznego wykrywania i dodawania przy wykorzystaniu usług katalogowych. Wszystkie hosty i urządzenia należące do wybranej domeny powinny być automatycznie dodane do CSB wraz z zainstalowanym na nich oprogramowaniem. Drugi i trzeci sposób natomiast ma umożliwiać użytkownikowi/administratorowi dodanie urządzeń/hostów/oprogramowania nie należących do domeny poprzez “ręczne” wpisanie informacji (wypełnienie formularza) lub wczytanie pliku w formacie CSV posiadającego usystematyzowaną strukturę. Moduł inwentaryzacji musi być ściśle skorelowany (powiązany) z pozostałymi modułami systemu CSB.  5.2 Gromadzenie pełnych informacji na temat urządzeń (tj. nazwa hosta, adres IP, główny użytkownik) jak i oprogramowania (nazwa, wersja)  Informacje o urządzeniach/hostach/oprogramowaniu, które muszą znaleźć się zarówno w formularzu jak i pliku CSV to m.in. dla hosta/urządzenia: nazwa, adres IP, przypisany użytkownik, typ urządzenia/hosta oraz lista zainstalowanego na nim oprogramowania wraz z wersjami. Przy wprowadzaniu “ręcznym” system musi umożliwiać użytkownikowi/administratorowi wybór nazwy i wersji oprogramowania z listy znajdującej się bazie CVE, bądź wpisanie własnych wartości.  5.3.  Generowanie raportu w formacie PDF, CSV zawierającego aktualne informację na temat urządzeń oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.  Moduł musi być wyposażony w funkcjonalności umożliwiającą użytkownikowi/administratorowi wygenerowania raportów z całej dodanej w systemie CSB infrastruktury sieciowej. Raporty powinny być generowane w co najmniej dwóch formatach tj. PDF i CSV oraz powinny zawierać wszystkie istotne informację na temat urządzenia/hosta/oprogramowania m. in takie jak: nazwa, adres, główny użytkownik, lista oprogramowania wraz z wersjami. Ponadto raport musi zawierać m.in. datę i godzinę wygenerowania, nazwę jednostki organizacyjnej oraz imię i nazwisko osoby generującej raport. Dokładny wzór (wizualny) generowanego raportu zostanie ustalony przez zamawiającego w trakcie realizacji zamówienia. Moduł musi umożliwiać generowanie raportów zarówno z całości jak i z odfiltrowanych urządzeń/hostów/oprogramowania. Użytkownik/Administrator musi mieć możliwość odfiltrowania informacji według co najmniej takich kategorii jak: nazwa użytkownika, grupa urządzeń, dowolnie wpisana fraza. |  |
| **MODUŁ ZGŁASZANIA INCYDENTÓW (e-mail, system help-deskowy)** | 6.1. Integracja z systemem tiketowym.  System CSB musi w prosty i intuicyjny sposób umożliwiać użytkownikowi/administratorowi integrację z systemem typu: help-desk. Integracja powinna odbywać się poprzez ustawienie w konfiguracji CSB odpowiedniego adresu e-mail systemu help-deskowego, na który będą wysyłane zgłoszenia dotyczące problemów. Wysyłanie wiadomości ma się odbywać automatycznie po wybraniu przez użytkownika/administratora konkretnego zdarzenia w systemie CSB. Wiadomość e-mail powinna zwierać minimum nazwę jednostki organizacyjnej wysyłającej zgłoszenie, treść zgłoszenia oraz dane zgłaszającego: Imię Nazwisko, adres e-mail, numer telefonu.  6.2.  Zgłaszanie incydentu/problemu, który został namierzony przez system.  Moduł zgłaszania incydentu powinien być ściśle powiązany z modułem monitoringu zasobów, a dokładniej z funkcjonalnością wyświetlającą zidentyfikowane na urządzeniach/hostach problemy. Użytkownik/Administrator systemu powinien posiadać możliwość wyboru problemu namierzonego przez CSB i automatycznego zgłoszenia go do help-desk, poprzez wybranie np. przycisku “Zgłoś Problem”. Po wybraniu opcji zgłoszenia system powinien automatycznie wysyłać do systemu tiketowego zgłoszenie zawierające pełne informacje dotyczące wybranego problemu.  6.3.  Bezpośrednie zgłaszane zagrożeń/cyberataków do CSIRT NASK.  System powinien umożliwiać generowanie co najmniej pliku w formacie pdf ze zgłoszeniem zagrożenia/incydentu/ cyberataku zgodnego z formularzem udostępnianym przez NASK. |  |
| **MODUŁ ZGŁASZANIA INCYDENTÓW (e-mail, system help-deskowy)** | 7.1. Wykrywanie zagrożeń na podstawie powszechnie znanych taktyk i technik wykorzystywanych przez cyberprzestępców udostępnione w ogólnodostępnej bazie danych MITRE ATT&CK.  System musi umożliwiać użytkownikowi/administratorowi włączenie reguł sprawdzających, czy w jego infrastrukturze sieciowej nie zostały zastosowane taktyki i techniki różnego rodzaju cyberataków. System musi być zintegrowany z powszechnie dostępną bazą danych MITRE ATT&CK zawierającą zbiór taktyk i technik zaobserwowanych przez specjalistów na całym świecie. System powinien posiadać wbudowane reguły umożliwiające wykrycie wielu zagrożeń opisanych w matrycy MITRE ATT&CK, system powinien wskazywać użytkownikowi, przed jakiego rodzaju taktykami i technikami jest chronione jego środowisko IT. System musi pokazywać ilość wbudowanych w nim reguł wraz z ilością włączonych reguł. Użytkownik/Administrator systemu musi mieć możliwość sprawdzenia w systemie ile reguł dotyczących konkretnej techniki jest włączonych, a ile jeszcze pozostało do wyłączenia. System musi pokazywać pokrycie matrycy MITRE ATT&CK ilościom włączonych/wyłączonych reguł wykrywających cyberzagrożenia.  7.2.  Kategoryzacja oraz prezentacja wykrytych zagrożeń  System musi umożliwiać użytkownikowi/administratorowi sprawdzenie zagrożeń wykrytych na poszczególnych hostach/urządzeniach zinwentaryzowanych w module inwentaryzacji. Wykryte w systemie zagrożenia musza zawierać informację na temat: daty i czasu ich wystąpienia, rodzaju/treści oraz poziomu istotności. System powinien kategoryzować zagrożenia w co najmniej czterostopniowej skali: poziom zagrożenia niski, średni, wysoki, krytyczny.  7.3.  Historia wykrytych zagrożeń  System musi posiadać możliwość sprawdzenia historii występowania zagrożeń na hostach/urządzeniach. System musi być wyposażony w rozbudowaną wyszukiwarkę hostów i zagrożeń umożliwiającą między innymi: wyszukanie hosta po nazwie, adresie IP, kategorii/priorytetów, daty wykrycia (przedziału czasowego).  7.4.  Wsparcie/automatyczna ochrona po wykryciu zagrożenia  System musi posiadać możliwość włączenia “automatycznej ochrony” w wybrane dni tygodnia i w wybranych godzinach. Użytkownik/administrator musi mieć możliwość ustawienia automatycznej ochrony przed wybranymi taktykami i technikami działań cyberprzestępców poza godzinami jego pracy. System musi mieć możliwość ustawienia reakcji na wykrycie zagrożenia w zależności od wybranego poziomu istotności/priorytetu. Ponadto użytkownik/administrator musi mieć możliwość wybrania operacji/akcji z listy predefiniowanych operacji/akcji, która zostanie wykona w razie wykrycia zagrożenia o wybranym priorytecie. Lista operacji/akcji musi umożliwiać co najmniej wyłączenie/restart hosta/urządzenia na którym wykryto zagrożenie, przesłanie informacji o wystąpieniu zagrożenia do użytkownika/administratora przy wykorzystaniu poczty e-mail bądź bramki sms, blokowanie hosta na którym występuje zagrożenie. |  |
| **MODUŁ RAPORTÓW** | 8.1.  Tworzenie zestawień i raportów z danych pochodzących z pozostałych modułów  System musi posiadać możliwość tworzenie różnego rodzaju zestawień prowadzących do sporządzenia i wyeksportowania raportu w co najmniej dwóch formatach: csv, pdf. Podczas tworzenia zestawienia użytkownik/administrator musi mieć możliwość wyboru konkretnych hostów bądź grupy hostów, dla których tworzony jest raport. Użytkownik musi posiadać możliwość wyboru modułów oraz priorytetów zdarzeń w nich występujących. Ponadto użytkownik przez administrator musie mieć możliwość wyboru przedziału czasowego, dla którego zostanie wykonany raport. |  |
| **PANEL UŻYTKOWNIKA** | 9.1. Intuicyjny i przejrzysty panel użytkownika dostępny z dowolnej lokalizacji poprzez stronę www.  Panel użytkownika CSB powinien być przejrzysty i intuicyjny oraz wykonany przy wykorzystaniu najnowszych standardów i technologii stosowanych we współczesnych systemach informatycznych. Panel użytkownika/administratora sytemu musi być dostępny poprzez podanie odpowiedniego adresu w przeglądarce internetowej. Dostęp do panelu użytkownika musi być bezpieczny poprzez szyfrowanie (zabezpieczenie certyfikatem SSL) oraz tzw. białą listę adresów IP - która pozwala użytkownikowi/administratorowi systemu blokować dostęp z nie znajdujących się na niej adresów. Panel użytkownika powinien również spełniać wymagania związane z dostępnością̨ serwisów użyteczności publicznej dla osób z niepełnosprawnościami - WCAG 2.1 AA.  9.2. Wizualizacja statystyk zdarzeń i logów  Panel użytkownika CSB, powinien posiadać elementy umożliwiające prezentację statystyk zdarzeń i logów w sposób zrozumiały, ułatwiający analizę działania środowiska IT pod kątem cyberbezpieczeństwa. Wizualizacja statystyk zdarzeń i logów powinna dotyczyć przede wszystkim ilości “nowych” zdarzeń zarejestrowanych w systemie z podziałem na ich kategorię. Natomiast sposób prezentacji samych logów i zdarzeń musi być przejrzysty jasno podkreślający sklasyfikowanie zdarzenia czy wpisu do logów. Zdarzenia i logi powinny w systemie być wyświetlane w kolejności od najnowszych do najstarszych z możliwości odfiltrowania zakresu czasowego ich prezentowania.  9.3. Wykresy zdefiniowanych parametrów zasobowych aktualizowane na „żywo”.  Wykresy prezentujące parametry zasobów urządzeń/hostów powinny być aktualizowane w systemie na “żywo”, a dokładnie w zależności od ustaleń z zleceniodawcą system musi aktualizować wykresy w określonych odstępach czasowych (co najmniej, co minutę).  9.4. Filtrowanie wyświetlanych danych wg. hostów, oprogramowania, kategorii zdarzeń itd.  Panel użytkownika powinien być tak zaprojektowany, aby użytkownik/administrator w sposób intuicyjny mógł filtrować istotne dla niego informacje dotyczące zarówno obciążeń zasobów, zdarzeń (problemów, ostrzeżeń), czy logów. Panel użytkownika musi być wyposażony w wyszukiwarkę umożliwiająca filtrowanie informacji wg. m.in. nazwy hosta/urządzenia, nazwy oprogramowania czy kategorii zdarzeń i logów. Wyszukiwarka w panelu użytkownika powinna znajdować się w widocznym miejscu i posiadać precyzyjnie oznaczone możliwości filtrowania. Użytkownik/Administrator powinien mieć możliwość nakładania na siebie różnych filtrów.  9.5. Intuicyjny panel zarządzania regułami i definiowania “customowych” logów.    Panel użytkownika powinien być wyposażony w przejrzysty i intuicyjny panel zarządzania regułami (akcjami), na podstawie których użytkownik/administrator informowany jest o zaistniałym w środowisku IT problemie. W panelu tym musi znaleźć się między innymi lista już zdefiniowanych reguł z możliwością ich usunięcia i edycji oraz opcja umożliwiająca dodanie nowej reguły. Reguły w panelu użytkownika powinny być dodawane przy wykorzystaniu przejrzystego i intuicyjnego formularza, w którym użytkownik/administrator musi podać nazwę reguły, dodać warunku oraz wybrać rodzaj operacji, która zostanie wykonana, gdy warunki będą spełnione. Użytkownik/administrator CSB musi mieć możliwość wyboru zarówno warunków, reguł jak i operacji z udostępnionych w systemie opcji. Ponad to panel użytkownika musi być wyposażony w panel zarządzania “customowymi” logami, w którym podobnie jak w przypadku reguł, użytkownik/administrator może wyświetlić listę zdefiniowanych “customlogów” wraz z możliwością ich usunięcia, edycji oraz zdefiniowania nowych. Dodanie do systemu “customlogów” musi być intuicyjne i ma polegać na podaniu unikalnej nazwy definiowanych logów, jego ścieżki (lub ścieżek) dostępu oraz nazwy hosta lub grupy hostów, których ma on dotyczyć. |  |

1. **Serwer 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Obudowa** | Typu RACK, wysokość nie więcej niż 1U;  Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable;  Możliwość zainstalowania 8 dysków twardych hot plug 2,5”;  Opcjonalne fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;  Zainstalowane 8 szt. dysków SSD SATA 1,92 GB Hot-Plug, dyski skonfigurowane w RAID-10 podłączone do sprzętowego kontrolera RAID;  Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray |  |
| **Płyta główna** | Dwuprocesorowa;  Wyprodukowana i zaprojektowana przez producenta serwera;  Możliwość instalacji procesorów 60-rdzeniowych;  Moduł TPM 2.0;  4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5;  Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH;  32 gniazda pamięci RAM;  Obsługa 8 TB pamięci operacyjnej RAM DDR4;  Wsparcie dla technologii:  Memory Scrubbing;  SDDC; ECC;  Memory Mirroring;  ADDDC;  Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.  BIOS UEFI w specyfikacji 2.7. |  |
| **Procesory** | Min Dwa procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86\_64;osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 258 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla dowolnego serwera z oferty producenta. |  |
| **Pamięć RAM** | *Min 256 GB pamięci RAM;*  *DDR5 Registered 4800MT/s;* |  |
| **Kontrolery LAN** | Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:  Min 5x 1G Base-T;  Min 2x 10Gbit SFP+, porty obsadzone modułami SR LC;  Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;  Kontrolery I/O  Kontroler SAS RAID dla dysków wewnętrznych obsługujący RAID 0,1,10 5; |  |
| **Porty** | Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;  Min 2 porty USB 3.0 dostępne z tyłu serwera;  Min 2 porty USB 3.0 na panelu przednim;  Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;  Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera |  |
| **Zasilanie, chłodzenie** | Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W; Redundantne wentylatory hotplug |  |
| **Zarządzanie** | Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;  informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:  karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;  procesory CPU;  pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;  status karty zarządzającej serwera;  wentylatory;  bateria podtrzymująca ustawienia BIOS płyty głównej;  zasilacze;  system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:  Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;  Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;  Dostęp poprzez przeglądarkę Web, SSH;  Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;  Zarządzanie alarmami (zdarzenia poprzez SNMP);  Możliwość przejęcia konsoli tekstowej;  Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);  Obsługa serwerów proxy (autentykacja);  Obsługa VLAN;  Możliwość konfiguracji parametru Max. Transmission Unit (MTU);  Wsparcie dla protokołu SSDP;  Obsługa protokołów TLS 1.2, SSL v3;  Obsługa protokołu LDAP;  Integracja z HP SIM;  Synchronizacja czasu poprzez protokół NTP;  Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;  Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);  Wbudowana w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;  Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.  Wspierane OS  Microsoft Windows Server 2022, 2019;  VMWare vSphere 8.0;;  Suse Linux Enterprise Server 15; Red Hat Enterprise Linux 9, 8;  Microsoft Hyper-V Server 2019 |  |
| **Gwarancja** | Min 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.  Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu;  Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;  Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;  Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty). |  |
| **Dokumentacja, inne** | Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;  Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;  Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;  W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;  Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;  Należy dostarczyć i wstępnie skonfigurować system zarządzania infrastrukturą IT. Musi być możliwość monitorowania stanu środowiska IT minimum dla oferowanego serwerów. System zarządzania posiada jeden spójny interfejs GUI HTML do zarządzania całym oferowanym środowiskiem sprzętowym. System zarządzania opiera się o tzw. Virtual Appliance kompatybilny z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM. System zarządzania umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe. System zarządzania posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI. System zarządzania musi mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV.  Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;  Serwer musi być certyfikowany do pracy z systemem Ubuntu 22.04;  Zgodność z normami: CB, RoHS, WEEE, GS oraz CE |  |
| **Oprogramowanie** | 1. Licencja na serwerowy system operacyjny Windows SVR 2025 lub oprogramowanie równoważne - system musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie czterech instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Licencja musi w pełni pokrywać licencyjnie rdzenie fizyczne zaproponowanego serwera oraz liczbę użytkowników w ilości min 35 szt.   Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.   1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania  7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:    1. pozwalają na zmianę rozmiaru w czasie pracy systemu,    2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,    3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,    4. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:     1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,     2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o:     1. Login i hasło,     2. Karty z certyfikatami (smartcard),     3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:     1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,     2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:   Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.   * 1. Zdalna dystrybucja oprogramowania na stacje robocze.   2. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej   3. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:   Dystrybucję certyfikatów poprzez http  Konsolidację CA dla wielu lasów domeny,  Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.   * 1. Szyfrowanie plików i folderów.   2. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).   3. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.   4. Serwis udostępniania stron WWW.   5. Wsparcie dla protokołu IP w wersji 6 (IPv6),   6. Wsparcie dla algorytmów Suite B (RFC 4869),   7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,   8. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:   Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  Obsługi 4-KB sektorów dysków  Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)   1. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 2. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 4. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 5. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.   Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. |  |

1. **UPS 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Moc** | Min moc 3000VA/3000W, |  |
| **Parametry wejściowe** | * Napięcie: 230 V (1-fazowe), tolerancja 115 – 280 V * Częstotliwość: 50/60 Hz, tolerancja 40-70 Hz * Współczynnik mocy/THDi : > 0,99 / < 5 % |  |
| **Parametry wyjściowe:** | * Napięcie (czysty przebieg sinusoidalny): 230V * Częstotliwość: 50 Hz * Współczynnik mocy 1 * Sprawność: 94 % w trybie on-line * Przeciążalność: min. 105 % w sposób ciągły; 125 % przez 5 min; 150 % przez 60 s * Liczba i rodzaj gniazdek z utrzymaniem zasilania 1 x IEC320 C19 (16A), min 6 x IEC320 C13 (10A |  |
| **Bateria** | * Hermetyczne, bezobsługowe akumulatory typu VRLA AGM muszą zapewnić czas podtrzymania minimum 15 minut dla obciążenia 1200 W, minimum 4 min dla mocy 2700W * Bateria wbudowana w zasilacz UPS   obsługa min 10 zewnętrznych modułów bateryjnych |  |
| **Zasilacz UPS musi być zgodny z Normami** | * Parametry i topologia: IEC 62040-3 (VFI-SS-111) * Bezpieczeństwo: IEC/EN 62040-1 * Kompatybilność elektromagnetyczna IEC/EN 62040-2, kat. 2 * ESD: EN61000-4-2 poziom4, kryteria A * Podatność na wyemitowane zakłócenia: IEC/EN 61000-4-2 * Certyfikaty: CE lub inne równoważne   Stopień ochrony: IP20 |  |
| **Zasilacz UPS musi spełniać parametry środowiskowe, co najmniej takie jak:** | * Temperatura pracy od 0 °C do +40 °C (optymalne warunki żywotności baterii w zakresie temperatur od 15 °C do 25 °C) * Wilgotność: 0-95 % bez kondensacji * Poziom hałasu w odległości 1 m od przodu urządzenia: < 55 dB |  |
| **Parametry** | * Wymiary zasilacza UPS nie mogą być większe niż: szer. X głęb. x wys. (mm) 430 × 540 × 262 (+/- 10 mm) * Waga: 28,2 kg (+/- 0.5 kg) |  |
| **Komunikacja** | Zasilacz UPS musi być wyposażony w kartę SNMP, wbudowany port EPO (konfigurowalny NO/NC) oraz gniazda USB, RS232 i RS485. |  |

1. **System antywirusowy 35 USER licencja**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Administracja zdalna w chmurze** | 1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. 3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.   Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. |  |
|  | 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook 23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:  * tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące * tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, * tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, * tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. |  |
| **Ochrona serwera** | Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu  Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux  Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor  Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS  Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie  Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji  Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów  Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty  Dodatkowe wymagania dla ochrony serwerów Windows   1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.* 8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.   Dodatkowe wymagania dla ochrony serwerów Linux   1. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 2. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 3. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.   Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej |  |
| **Szyfrowanie** | 1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit. 2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.   Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI |  |
| **Ochrona urządzeń mobilnych opartych o system Android** | 1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi usunięcie zawartości urządzenia, przywrócenie urządzenie do ustawień fabrycznych, zablokowania urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS. |  |
| **Sandbox w chmurze** | 1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 2. Rozwiązanie musi wykorzystywać do działania chmurę producenta. 3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. 6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. 8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. 9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. 12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:   Czysty,  Podejrzany,  Bardzo podejrzany,  Szkodliwy.   1. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. 2. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.   Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia |  |
| **Moduł XDR** | 1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. 6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. 9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. 13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.   Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.   1. Konsola administracyjna musi mieć możliwość tagowania obiektów   Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershe |  |

1. **Serwer NAS 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Procesor** | Min Czterordzeniowy procesor Intel Xeon D-1521 z taktowaniem 2,4 GHz (maksymalnie 2,7 GHz z technologią Turbo Boost) lub równoważny |  |
| **budowana pamięć RAM** | Min 8 GB |  |
| **Maks. wielkość pamięci** | 64 GB |  |
| **Rodzaj pamięci** | DDR4 |  |
| **Liczba obsadzonych gniazd pamięci** | Min 1 |  |
| **Maks. liczba dysków** | Min 12 |  |
| **Typ dysku** | * HDD   SSD |  |
| **Ilość zainstalowanych dysków** | 12 x 4TB |  |
| **Format szerokości** | * 2,5'' (SFF)   3,5'' (LFF) |  |
| **Interfejs dysku** | SATA |  |
| **Obsługa hot-swap dysków** | Tak |  |
| **RAID** | Tak |  |
| **Poziomy RAID – min** | * 0 * 1 * 10 (1+0) * 5   6 |  |
| **Architektura sieci** | GigabitEthernet |  |
| **Interfejs sieciowy** | MIN 4 x 10/100/1000 Mbit/s |  |
| **Liczba wentylatorów** | MIN 4 |  |
| **Obudowa** | Max Rack 2U |  |
| **Gniazda rozszerzeń** | 2 x PCIe 3.0 x 8 |  |
| **Waga** | 14.5 kg z tolerancją -/+ 0,5 kg |  |
| **Wymiary** | Max 88 × 482 × 724 mm (z uchwytem serwera) z tolerancją na wymiarach -/+ 10 mm |  |

1. **UPS 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Moc** | Min moc 3000VA/3000W, |  |
| **Parametry wejściowe** | * Napięcie: 230 V (1-fazowe), tolerancja 115 – 280 V * Częstotliwość: 50/60 Hz, tolerancja 40-70 Hz   Współczynnik mocy/THDi : > 0,99 / < 5 % |  |
| **Parametry wyjściowe:** | * Napięcie (czysty przebieg sinusoidalny): 230V * Częstotliwość: 50 Hz * Współczynnik mocy 1 * Sprawność: 94 % w trybie on-line * Przeciążalność: min. 105 % w sposób ciągły; 125 % przez 5 min; 150 % przez 60 s   Liczba i rodzaj gniazdek z utrzymaniem zasilania 1 x IEC320 C19 (16A), min 6 x IEC320 C13 (10A |  |
| **Bateria** | * Hermetyczne, bezobsługowe akumulatory typu VRLA AGM muszą zapewnić czas podtrzymania minimum 15 minut dla obciążenia 1200 W, minimum 4 min dla mocy 2700W * Bateria wbudowana w zasilacz UPS   obsługa min 10 zewnętrznych modułów bateryjnych |  |
| **Zasilacz UPS musi być zgodny z Normami** | * Parametry i topologia: IEC 62040-3 (VFI-SS-111) * Bezpieczeństwo: IEC/EN 62040-1 * Kompatybilność elektromagnetyczna IEC/EN 62040-2, kat. 2 * ESD: EN61000-4-2 poziom4, kryteria A * Podatność na wyemitowane zakłócenia: IEC/EN 61000-4-2 * Certyfikaty: CE   Stopień ochrony: IP20 |  |
| **Zasilacz UPS musi spełniać parametry środowiskowe, co najmniej takie jak:** | * Temperatura pracy od 0 °C do +40 °C (optymalne warunki żywotności baterii w zakresie temperatur od 15 °C do 25 °C) * Wilgotność: 0-95 % bez kondensacji   Poziom hałasu w odległości 1 m od przodu urządzenia: < 55 dB |  |
| **Parametry** | * Wymiary zasilacza UPS nie mogą być większe niż: szer. x głęb. x wys. (mm) 430 × 540 × 262 * Waga: 28,2 kg |  |
| **Komunikacja** | Zasilacz UPS musi być wyposażony w kartę SNMP, wbudowany port EPO (konfigurowalny NO/NC) oraz gniazda USB, RS232 i RS485. |  |

1. **Urządzenie UTM 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Redundancja, monitoring i wykrywanie awarii** | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN.   System ma umożliwić agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |  |
| **Interfejsy, Dysk, Zasilanie** | 1. System realizujący funkcję Firewall musi dysponować minimum:   16 portami Gigabit Ethernet RJ-45.  8 gniazdami SFP 1 Gbps.   1. gniazdami SFP+ 10 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 4. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB. 5. System musi być wyposażony w zasilanie AC. |  |
| **Parametry wydajnościowe:** | 1. W zakresie Firewall’a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. 3. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 64 B. 4. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 1518 B. 5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps. 6. Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps. 7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.   Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps. |  |
| **Funkcje Systemu Bezpieczeństwa:** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów: SMTP, POP3 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL.   Analiza ruchu szyfrowanego protokołem SSH |  |
| **Polityki, Firewall** | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: 3. Translację jeden do jeden oraz jeden do wielu. 4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 5. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 6. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.   Amazon Web Services (AWS).  Microsoft Azure  Cisco ACI.  Google Cloud Platform (GCP).  Nuage Networks VSP.  OpenStack.  VMware vCenter (ESXi).  VMware NSX. |  |
| **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: 2. Wsparcie dla IKE v1 oraz v2. 3. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). 4. Obsługa protokołu Diffie-Hellman grup 19 i 20. 5. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. 6. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 7. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. 8. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. 9. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. 10. Mechanizm „Split tunneling” dla połączeń Client-to-Site. 11. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: 12. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. 13. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.   Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |  |
| **Routing i obsługa łączy WAN** | 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:   Routingu statycznego.  Policy Based Routingu.  Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |  |
| **Zarządzanie pasmem** | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.   System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
| **Ochrona przed malware** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.   System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |  |
| **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  |
| **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.   Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |  |
| **Kontrola WWW** | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.   W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |  |
| **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: 2. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. 3. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. 4. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 5. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.   Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |  |
| **Zarządzanie** | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.   Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  |
| **Logowanie** | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG |  |
| **Testy wydajnościowe oraz funkcjonalne** | 1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta. |  |
| **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  a)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy |  |
| **Gwarancja oraz wsparcie** | 1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie . 2. Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). |  |

1. **Przełącznik sieciowy 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| Warstwa przełączania | * L2   L3 |  |
| Architektura sieci | GigabitEthernet |  |
| Liczba portów 10/100/1000 Mbps | Min 48 |  |
| Liczba portów 10Gb | Min 4 |  |
| Liczba portów SFP+ | Min 4 |  |
| Przepustowość | Min 88 Gb/s |  |
| Prędkość przekazywania | Min 130.944 Mpps |  |
| Możliwość łączenia w stos | Min Tak |  |
| Bezpieczeństwo | Ochrona ESD / EMP: Powietrze: 16 kV, Kontakt: 12 kV |  |
| Typ obudowy | Rack |  |
| Zasilacz | Wewnętrzny |  |
| Pobór mocy | Max 60 W |  |
| Zasilanie | AC / DC, 60 W. |  |
| Wymiary | Max 442,4 x 285,4 x 43,7 mm z tolerancją +/- 20 mm |  |
| Waga | Max 4 kg z tolerancją 0,5 kg |  |
| Informacje o gwarancji | Min Gwarancja 36 miesięcy liczona od daty sprzedaży |  |

1. **Serwer z systemem operacyjnym dla GOPS w Czudcu 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Obudowa** | Typu RACK, wysokość nie więcej niż 1U;  Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable;  Możliwość zainstalowania 8 dysków twardych hot plug 2,5”;  Opcjonalne fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;  Zainstalowane 2 szt. dysków SSD SATA 480 GB Hot-Plug, dyski skonfigurowane 3 x dysków SSD SATA 1,92 TB Hot-Plug podłączone do sprzętowego kontrolera RAID;  Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray |  |
| Płyta główna | Dwuprocesorowa;  Wyprodukowana i zaprojektowana przez producenta serwera;  Możliwość instalacji procesorów 60-rdzeniowych;  Moduł TPM 2.0;  4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5;  Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH;  32 gniazda pamięci RAM;  Obsługa 8 TB pamięci operacyjnej RAM DDR4;  Wsparcie dla technologii:  Memory Scrubbing;  SDDC; ECC;  Memory Mirroring;  ADDDC;  Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.  BIOS UEFI w specyfikacji 2.7. |  |
| **Procesory** | Min jeden procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86\_64;osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 258 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla dowolnego serwera z oferty producenta. |  |
| **Pamięć RAM** | *Min 128 GB pamięci RAM;*  *DDR5 Registered 4800MT/s;* |  |
| Kontrolery LAN | Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:  Min 5x 1G Base-T;  Min 2x 10Gbit SFP+, porty obsadzone modułami SR LC;  Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;  Kontrolery I/O  Kontroler SAS RAID dla dysków wewnętrznych obsługujący RAID 0,1,10 5; |  |
| Porty | Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;  Min 2 porty USB 3.0 dostępne z tyłu serwera;  Min 2 porty USB 3.0 na panelu przednim;  Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;  Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera |  |
| Zasilanie, chłodzenie | Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W; Redundantne wentylatory hotplug |  |
| Zarządzanie | Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;  informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:  karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;  procesory CPU;  pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;  status karty zarządzającej serwera;  wentylatory;  bateria podtrzymująca ustawienia BIOS płyty głównej;  zasilacze;  system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:  Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;  Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;  Dostęp poprzez przeglądarkę Web, SSH;  Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;  Zarządzanie alarmami (zdarzenia poprzez SNMP);  Możliwość przejęcia konsoli tekstowej;  Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);  Obsługa serwerów proxy (autentykacja);  Obsługa VLAN;  Możliwość konfiguracji parametru Max. Transmission Unit (MTU);  Wsparcie dla protokołu SSDP;  Obsługa protokołów TLS 1.2, SSL v3;  Obsługa protokołu LDAP;  Integracja z HP SIM;  Synchronizacja czasu poprzez protokół NTP;  Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;  Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);  Wbudowana w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;  Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.  Wspierane OS  Microsoft Windows Server 2022, 2019;  VMWare vSphere 8.0;;  Suse Linux Enterprise Server 15;  Red Hat Enterprise Linux 9, 8;  Microsoft Hyper-V Server 2019 |  |
| Gwarancja | Min 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.  Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu;  Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;  Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;  Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty). |  |
| Dokumentacja, inne | Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;  Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;  Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;  W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;  Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;  Należy dostarczyć i wstępnie skonfigurować system zarządzania infrastrukturą IT. Musi być możliwość monitorowania stanu środowiska IT minimum dla oferowanego serwerów. System zarządzania posiada jeden spójny interfejs GUI HTML do zarządzania całym oferowanym środowiskiem sprzętowym. System zarządzania opiera się o tzw. Virtual Appliance kompatybilny z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM. System zarządzania umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe. System zarządzania posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI. System zarządzania musi mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV.  Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;  Serwer musi być certyfikowany do pracy z systemem Ubuntu 22.04;  Zgodność z normami: CB, RoHS, WEEE, GS oraz CE |  |
| **Oprogramowanie** | Licencja na serwerowy system operacyjny Windows SVR 2025 lub oprogramowanie równoważne - system musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie czterech instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Licencja musi w pełni pokrywać licencyjnie rdzenie fizyczne zaproponowanego serwera oraz liczbę użytkowników w ilości min 10 szt.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.  Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.  Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.  Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania  7000 maszyn wirtualnych.  Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.  Wbudowane wsparcie instalacji i pracy na wolumenach, które:   * 1. pozwalają na zmianę rozmiaru w czasie pracy systemu,   2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,   3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,   4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).   Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  Dostępne dwa rodzaje graficznego interfejsu użytkownika:   * 1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,   2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.   Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.  Mechanizmy logowania w oparciu o:   * 1. Login i hasło,   2. Karty z certyfikatami (smartcard),   3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),   Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..  Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).  Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:   * 1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,   2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:   Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.   * 1. Zdalna dystrybucja oprogramowania na stacje robocze.   2. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej   3. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:   Dystrybucję certyfikatów poprzez http  Konsolidację CA dla wielu lasów domeny,  Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.   * 1. Szyfrowanie plików i folderów.   2. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).   3. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.   4. Serwis udostępniania stron WWW.   5. Wsparcie dla protokołu IP w wersji 6 (IPv6),   6. Wsparcie dla algorytmów Suite B (RFC 4869),   7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,   8. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:   Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  Obsługi 4-KB sektorów dysków  Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)  Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).  Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.  Zorganizowany system szkoleń i materiały edukacyjne w języku polskim |  |

1. **Zasilacze awaryjne UPS do stanowisk komputerowych dla GOPS w Czudcu 10 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Moc pozorna** | Min 600 VA |  |
| **Moc czynna** | Min 360 W |  |
| **Czas podtrzymania (obciążenie 100%)** | Min 3 min |  |
| **Czas ładowania** | Max 4h |  |
| **Typ obudowy** | TOWER |  |
| **Zabezpieczenia / filtry** | Nadmierne rozładowanie  Przeciw przeciążeniowe |  |
| **Funkcje specjalne** | - Zimny start - Układ automatycznej regulacji napięcia (AVR) - Sinus podczas pracy na baterii **Diody informujące o:** - Ładowaniu baterii - Przeciążeniu UPSa - Słabej baterii - Przeciążeniu - Koniecznej wymianie baterii - Awarii akumulatora |  |
| **Porty zasilania wy.** | 2 x typ C/F (Schuko) |  |
| **Wymagania środowiskowe** | - Temperatura pracy: od 0 do 40 stopni C - Temperatura przechowywania: od -20 do 50 stopni C - Wilgotność otoczenia pracy/przechowywania: 0 - 90% (bez kondensacji) |  |
| **Pozostałe parametry** | - Min moc rzeczywista: 360W - Min Złącze wejściowe: kabel z wtykiem Schuko (10A) - Min czas podtrzymania przy obciążeniu 50%: 6 minut |  |

1. **Serwer NAS dla GOPS w Czudcu 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Procesor** | Liczba procesorów: 1 Architektura procesora: 64-bit Częstotliwość procesora: 4-core 2.0 (podstawowy) / 2.7 (turbo) GHz Mechanizm szyfrowania sprzętowego (AES-NI) lub równoważny |  |
| **budowana pamięć RAM** | Min 2GB |  |
| **Maks. wielkość pamięci** | 6 GB |  |
| **Rodzaj pamięci** | DDR4 |  |
| **Liczba obsadzonych gniazd pamięci** | Min 1 |  |
| **Maks. liczba dysków** | 4 |  |
| **Typ dysku** | * HDD   SSD |  |
| **Ilośc zainstalowanych dysków** | 4 x 4TB |  |
| **Format szerokości** | * 2,5'' (SFF)   3,5'' (LFF) |  |
| **Interfejs dysku** | SATA |  |
| **Obsługa hot-swap dysków** | Tak |  |
| **RAID** | Tak |  |
| **Poziomy RAID – min** | * 0 * 1 * 10 (1+0) * 5 * 6   JBOD |  |
| **Architektura sieci** | GigabitEthernet |  |
| **Interfejs sieciowy** | Min 2 x 10/100/1000 Mbit/s |  |
| **Gniazda rozszerzeń** | MIN 2 x M.2 |  |
| **Gniazda we/wy** | * Min 2 x RJ-45 LAN   MIN 2 x USB 3.0 |  |
| **Liczba wentylatorów** | MIN 2 |  |
| **Obudowa** | Tower |  |
| **Zasilanie** | * MAX Zasilacz: 90 W * Napięcie wejściowe zasilania prądem zmiennym: 100V to 240V AC * Zużycie energii: 28.3 W (dostęp); 8.45 W (hibernacja dysków twardych) |  |

1. **UTM wraz ze wsparciem technicznym oraz subskrypcjami dla GOPS w Czudcu 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Redundancja, monitoring i wykrywanie awarii** | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN.   System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |  |
| **Interfejsy, Dysk, Zasilanie** | 1. System realizujący funkcję Firewall musi dysponować minimum: 10 portami Gigabit Ethernet RJ-45.   1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB.   System musi być wyposażony w zasilanie AC. |  |
| **Parametry wydajnościowe:** | 1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 750 Mbps.   Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 650 Mbps. |  |
| **Funkcje Systemu Bezpieczeństwa:** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów: SMTP, POP3 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL.   Analiza ruchu szyfrowanego protokołem SSH |  |
| **Polityki, Firewall** | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: 3. Translację jeden do jeden oraz jeden do wielu. 4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 5. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 6. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.   Amazon Web Services (AWS).  Microsoft Azure  Cisco ACI.  Google Cloud Platform (GCP).  Nuage Networks VSP.  OpenStack.  VMware vCenter (ESXi).  VMware NSX. |  |
| **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: 2. Wsparcie dla IKE v1 oraz v2. 3. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). 4. Obsługa protokołu Diffie-Hellman grup 19 i 20. 5. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. 6. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 7. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. 8. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. 9. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. 10. Mechanizm „Split tunneling” dla połączeń Client-to-Site. 11. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: 12. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. 13. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.   Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |  |
| **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie powinno zapewniać obsługę:  Routingu statycznego.  Policy Based Routingu.  Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |  |
| **Zarządzanie pasmem** | System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.  Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.  System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
| **Ochrona przed malware** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.   System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |  |
| **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  |
| **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.   Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |  |
| **Kontrola WWW** | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.   W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |  |
| **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: 2. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. 3. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. 4. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 5. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.   Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |  |
| **Zarządzanie** | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.   Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  |
| **Logowanie** | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.   Musi istnieć możliwość logowania do serwera SYSLOG |  |
| **Testy wydajnościowe oraz funkcjonalne** | Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta. |  |
| **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  a)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy |  |
| **Gwarancja oraz wsparcie** | System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie .  Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). |  |

1. **Serwer z systemem operacyjnym dla ZEAS w Czudcu 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Obudowa** | Typu RACK, wysokość nie więcej niż 1U;  Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable;  Możliwość zainstalowania 8 dysków twardych hot plug 2,5”;  Opcjonalne fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;  Zainstalowane 2 szt. dysków SSD SATA 480 GB Hot-Plug, dyski skonfigurowane 3 x dysków SSD SATA 1,92 TB Hot-Plug podłączone do sprzętowego kontrolera RAID;  Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray |  |
| Płyta główna | Dwuprocesorowa;  Wyprodukowana i zaprojektowana przez producenta serwera;  Możliwość instalacji procesorów 60-rdzeniowych;  Moduł TPM 2.0;  4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5;  Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH;  32 gniazda pamięci RAM;  Obsługa 8 TB pamięci operacyjnej RAM DDR4;  Wsparcie dla technologii:  Memory Scrubbing;  SDDC; ECC;  Memory Mirroring;  ADDDC;  Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.  BIOS UEFI w specyfikacji 2.7. |  |
| **Procesory** | Min jeden procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86\_64;osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 258 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla dowolnego serwera z oferty producenta. |  |
| **Pamięć RAM** | *Min 128 GB pamięci RAM;*  *DDR5 Registered 4800MT/s;* |  |
| Kontrolery LAN | Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:  Min 5x 1G Base-T;  Min 2x 10Gbit SFP+, porty obsadzone modułami SR LC;  Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;  Kontrolery I/O  Kontroler SAS RAID dla dysków wewnętrznych obsługujący RAID 0,1,10 5; |  |
| Porty | Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;  Min 2 porty USB 3.0 dostępne z tyłu serwera;  Min 2 porty USB 3.0 na panelu przednim;  Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;  Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera |  |
| Zasilanie, chłodzenie | Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W; Redundantne wentylatory hotplug |  |
| Zarządzanie | Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;  informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:  karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;  procesory CPU;  pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;  status karty zarządzającej serwera;  wentylatory;  bateria podtrzymująca ustawienia BIOS płyty głównej;  zasilacze;  system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:  Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;  Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;  Dostęp poprzez przeglądarkę Web, SSH;  Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;  Zarządzanie alarmami (zdarzenia poprzez SNMP);  Możliwość przejęcia konsoli tekstowej;  Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);  Obsługa serwerów proxy (autentykacja);  Obsługa VLAN;  Możliwość konfiguracji parametru Max. Transmission Unit (MTU);  Wsparcie dla protokołu SSDP;  Obsługa protokołów TLS 1.2, SSL v3;  Obsługa protokołu LDAP;  Integracja z HP SIM;  Synchronizacja czasu poprzez protokół NTP;  Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;  Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);  Wbudowana w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;  Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.  Wspierane OS  Microsoft Windows Server 2022, 2019;  VMWare vSphere 8.0;;  Suse Linux Enterprise Server 15;  Red Hat Enterprise Linux 9, 8;  Microsoft Hyper-V Server 2019 |  |
| Gwarancja | Min 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.  Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu;  Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;  Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;  Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty). |  |
| Dokumentacja, inne | Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;  Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;  Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;  W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;  Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;  Należy dostarczyć i wstępnie skonfigurować system zarządzania infrastrukturą IT. Musi być możliwość monitorowania stanu środowiska IT minimum dla oferowanego serwerów. System zarządzania posiada jeden spójny interfejs GUI HTML do zarządzania całym oferowanym środowiskiem sprzętowym. System zarządzania opiera się o tzw. Virtual Appliance kompatybilny z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM. System zarządzania umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe. System zarządzania posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI. System zarządzania musi mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV.  Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;  Serwer musi być certyfikowany do pracy z systemem Ubuntu 22.04;  Zgodność z normami: CB, RoHS, WEEE, GS oraz CE |  |
| **Oprogramowanie** | Licencja na serwerowy system operacyjny Windows SVR 2025 lub oprogramowanie równoważne - system musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie czterech instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Licencja musi w pełni pokrywać licencyjnie rdzenie fizyczne zaproponowanego serwera oraz liczbę użytkowników w ilości min 10 szt.  Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.  Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.  Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.  Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania  7000 maszyn wirtualnych.  Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.  Wbudowane wsparcie instalacji i pracy na wolumenach, które:   * 1. pozwalają na zmianę rozmiaru w czasie pracy systemu,   2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,   3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,   4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).   Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  Dostępne dwa rodzaje graficznego interfejsu użytkownika:   * 1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,   2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.   Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.  Mechanizmy logowania w oparciu o:   * 1. Login i hasło,   2. Karty z certyfikatami (smartcard),   3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),   Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..  Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).  Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:   * 1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,   2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:   Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.   * 1. Zdalna dystrybucja oprogramowania na stacje robocze.   2. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej   3. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:   Dystrybucję certyfikatów poprzez http  Konsolidację CA dla wielu lasów domeny,  Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.   * 1. Szyfrowanie plików i folderów.   2. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).   3. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.   4. Serwis udostępniania stron WWW.   5. Wsparcie dla protokołu IP w wersji 6 (IPv6),   6. Wsparcie dla algorytmów Suite B (RFC 4869),   7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,   8. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:   Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  Obsługi 4-KB sektorów dysków  Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)  Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).  Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |  |

1. **Zasilacze awaryjne UPS do stanowisk komputerowych dla ZEAS w Czudcu 10 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Moc pozorna** | Min 600 VA |  |
| **Moc czynna** | Min 360 W |  |
| **Czas podtrzymania (obciążenie 100%)** | Min 3 min |  |
| **Czas ładowania** | Max 4h |  |
| **Typ obudowy** | TOWER |  |
| **Zabezpieczenia / filtry** | Nadmierne rozładowanie  Przeciw przeciążeniowe |  |
| **Funkcje specjalne** | - Zimny start - Układ automatycznej regulacji napięcia (AVR) - Sinus podczas pracy na baterii **Diody informujące o:** - Ładowaniu baterii - Przeciążeniu UPSa - Słabej baterii - Przeciążeniu - Koniecznej wymianie baterii - Awarii akumulatora |  |
| **Porty zasilania wy.** | 2 x typ C/F (Schuko) |  |
| **Wymagania środowiskowe** | - Temperatura pracy: od 0 do 40 stopni C - Temperatura przechowywania: od -20 do 50 stopni C - Wilgotność otoczenia pracy/przechowywania: 0 - 90% (bez kondensacji) |  |
| **Pozostałe parametry** | - Min moc rzeczywista: 360W - Min Złącze wejściowe: kabel z wtykiem Schuko (10A) - Min czas podtrzymania przy obciążeniu 50%: 6 minut |  |

1. **Zarządzany przełącznik sieciowy dla ZEAS w Czudcu 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| Warstwa przełączania | L2  L3 |  |
| Architektura sieci | GigabitEthernet |  |
| Liczba portów 10/100/1000 Mbps | Min 48 |  |
| Liczba portów 10Gb | Min 4 |  |
| Liczba portów SFP+ | Min 4 |  |
| Przepustowość | Min 88 Gb/s |  |
| Prędkość przekazywania | Min 130.944 Mpps |  |
| Możliwość łączenia w stos | Min Tak |  |
| Bezpieczeństwo | Ochrona ESD / EMP: Powietrze: 16 kV, Kontakt: 12 kV |  |
| Typ obudowy | Rack |  |
| Zasilacz | Wewnętrzny |  |
| Pobór mocy | Max 60 W |  |
| Zasilanie | AC / DC, 60 W. |  |
| Wymiary | Max 442,4 x 285,4 x 43,7 mm |  |
| Waga | Max 4 kg |  |
| Informacje o gwarancji | Min Gwarancja 36 miesięcy liczona od daty sprzedaży |  |

1. **Serwer NAS dla ZEAS w Czudcu 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Procesor** | Min Intel Celeron J4125 Liczba procesorów: 1 Architektura procesora: 64-bit Częstotliwość procesora: 4-core 2.0 (podstawowy) / 2.7 (turbo) GHz Mechanizm szyfrowania sprzętowego (AES-NI)  lub równoważny |  |
| **budowana pamięć RAM** | Min 2GB |  |
| **Maks. wielkość pamięci** | 6 GB |  |
| **Rodzaj pamięci** | DDR4 |  |
| **Liczba obsadzonych gniazd pamięci** | Min 1 |  |
| **Maks. liczba dysków** | 4 |  |
| **Typ dysku** | * HDD   SSD |  |
| **Ilośc zainstalowanych dysków** | 4 x 4TB |  |
| **Format szerokości** | * 2,5'' (SFF)   3,5'' (LFF) |  |
| **Interfejs dysku** | SATA |  |
| **Obsługa hot-swap dysków** | Tak |  |
| **RAID** | Tak |  |
| **Poziomy RAID – min** | * 0 * 1 * 10 (1+0) * 5 * 6   JBOD |  |
| **Architektura sieci** | GigabitEthernet |  |
| **Interfejs sieciowy** | Min 2 x 10/100/1000 Mbit/s |  |
| **Gniazda rozszerzeń** | MIN 2 x M.2 |  |
| **Gniazda we/wy** | * Min 2 x RJ-45 LAN   MIN 2 x USB 3.0 |  |
| **Liczba wentylatorów** | MIN 2 |  |
| **Obudowa** | Tower |  |
| **Zasilanie** | * MAX Zasilacz: 90 W * Napięcie wejściowe zasilania prądem zmiennym: 100V to 240V AC   Zużycie energii: 28.3 W (dostęp); 8.45 W (hibernacja dysków twardych) |  |
| **Waga** | * Max 2.18 kg z tolerancją +/-0,5 kg |  |
| **Wymiary** | * Max 166 x 199 x 223 mm z tolerancją +/- 15 mm |  |

1. **UTM wraz ze wsparciem technicznym oraz subskrypcjami dla ZEAS w Czudcu 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Redundancja, monitoring i wykrywanie awarii** | W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.  Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.  Monitoring stanu realizowanych połączeń VPN.  System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |  |
| **Interfejsy, Dysk, Zasilanie** | 1. System realizujący funkcję Firewall musi dysponować minimum: 10 portami Gigabit Ethernet RJ-45.   1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB.   System musi być wyposażony w zasilanie AC. |  |
| **Parametry wydajnościowe:** | * 1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.   2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.   3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.   4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.   5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.   6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 750 Mbps.   7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 650 Mbps. |  |
| **Funkcje Systemu Bezpieczeństwa:** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów: SMTP, POP3 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. Analiza ruchu szyfrowanego protokołem SSH |  |
| **Polityki, Firewall** | * 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  1. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: 2. Translację jeden do jeden oraz jeden do wielu. 3. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 4. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.    1. Amazon Web Services (AWS).    2. Microsoft Azure    3. Cisco ACI.    4. Google Cloud Platform (GCP).    5. Nuage Networks VSP.    6. OpenStack.    7. VMware vCenter (ESXi).    8. VMware NSX. |  |
| **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: 2. Wsparcie dla IKE v1 oraz v2. 3. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). 4. Obsługa protokołu Diffie-Hellman grup 19 i 20. 5. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. 6. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 7. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. 8. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. 9. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. 10. Mechanizm „Split tunneling” dla połączeń Client-to-Site. 11. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: 12. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. 13. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.   Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |  |
| **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie powinno zapewniać obsługę:  Routingu statycznego.  Policy Based Routingu.  Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |  |
| **Zarządzanie pasmem** | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
| **Ochrona przed malware** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |  |
| **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  |
| **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |  |
| **Kontrola WWW** | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |  |
| **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: 2. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. 3. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. 4. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 5. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 6. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |  |
| **Zarządzanie** | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  |
| **Logowanie** | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG |  |
| **Testy wydajnościowe oraz funkcjonalne** | Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta. |  |
| **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy |  |
| **Gwarancja oraz wsparcie** | System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie .  Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). |  |

1. **Zasilacze awaryjne UPS do stanowisk komputerowych dla ZWK w Czudcu 9 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Moc pozorna** | Min 600 VA |  |
| **Moc czynna** | Min 360 W |  |
| **Czas podtrzymania (obciążenie 100%)** | Min 3 min |  |
| **Czas ładowania** | Max 4h |  |
| **Typ obudowy** | TOWER |  |
| **Zabezpieczenia / filtry** | Nadmierne rozładowanie  Przeciw przeciążeniowe |  |
| **Funkcje specjalne** | - Zimny start - Układ automatycznej regulacji napięcia (AVR) - Sinus podczas pracy na baterii **Diody informujące o:** - Ładowaniu baterii - Przeciążeniu UPSa - Słabej baterii - Przeciążeniu - Koniecznej wymianie baterii - Awarii akumulatora |  |
| **Porty zasilania wy.** | 2 x typ C/F (Schuko) |  |
| **Wymagania środowiskowe** | - Temperatura pracy: od 0 do 40 stopni C - Temperatura przechowywania: od -20 do 50 stopni C - Wilgotność otoczenia pracy/przechowywania: 0 - 90% (bez kondensacji) |  |
| **Pozostałe parametry** | - Min moc rzeczywista: 360W - Min Złącze wejściowe: kabel z wtykiem Schuko (10A) - Min czas podtrzymania przy obciążeniu 50%: 6 minut |  |

1. **Zarządzany przełącznik sieciowy dla ZWK w Czudcu 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Warstwa przełączania** | L2  L3 |  |
| **Architektura sieci** | GigabitEthernet |  |
| **Liczba portów 10/100/1000 Mbps** | Min 48 |  |
| **Liczba portów 10Gb** | Min 4 |  |
| **Liczba portów SFP+** | Min 4 |  |
| **Przepustowość** | Min 88 Gb/s |  |
| **Prędkość przekazywania** | Min 130.944 Mpps |  |
| **Możliwość łączenia w stos** | Min Tak |  |
| **Bezpieczeństwo** | Ochrona ESD / EMP: Powietrze: 16 kV, Kontakt: 12 kV |  |
| **Typ obudowy** | Rack |  |
| **Zasilacz** | Wewnętrzny |  |
| **Pobór mocy** | Max 60 W |  |
| **Zasilanie** | AC / DC, 60 W. |  |
| **Wymiary** | Max 442,4 x 285,4 x 43,7 mm |  |
| **Waga** | Max 4 kg |  |
| **Informacje o gwarancji** | Min Gwarancja 36 miesięcy liczona od daty sprzedaży |  |

1. **Serwer NAS dla ZWK w Czudcu 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Procesor** | Liczba procesorów: 1 Architektura procesora: 64-bit Częstotliwość procesora: 4-core 2.0 (podstawowy) / 2.7 (turbo) GHz Mechanizm szyfrowania sprzętowego (AES-NI) |  |
| **budowana pamięć RAM** | Min 2GB |  |
| **Maks. wielkość pamięci** | 6 GB |  |
| **Rodzaj pamięci** | DDR4 |  |
| **Liczba obsadzonych gniazd pamięci** | Min 1 |  |
| **Maks. liczba dysków** | 4 |  |
| **Typ dysku** | * HDD   SSD |  |
| **Ilośc zainstalowanych dysków** | 4 x 4TB |  |
| **Format szerokości** | * 2,5'' (SFF)   3,5'' (LFF) |  |
| **Interfejs dysku** | SATA |  |
| **Obsługa hot-swap dysków** | Tak |  |
| **RAID** | Tak |  |
| **Poziomy RAID – min** | * 0 * 1 * 10 (1+0) * 5 * 6   JBOD |  |
| **Architektura sieci** | GigabitEthernet |  |
| **Interfejs sieciowy** | Min 2 x 10/100/1000 Mbit/s |  |
| **Gniazda rozszerzeń** | MIN 2 x M.2 |  |
| **Gniazda we/wy** | * Min 2 x RJ-45 LAN   MIN 2 x USB 3.0 |  |
| **Liczba wentylatorów** | MIN 2 |  |
| **Obudowa** | Tower |  |
| **Zasilanie** | * MAX Zasilacz: 90 W * Napięcie wejściowe zasilania prądem zmiennym: 100V to 240V AC   Zużycie energii: 28.3 W (dostęp); 8.45 W (hibernacja dysków twardych) |  |

1. **UTM wraz ze wsparciem technicznym oraz subskrypcjami dla ZWK w Czudcu 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Redundancja, monitoring i wykrywanie awarii** | * 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.   2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.   3. Monitoring stanu realizowanych połączeń VPN.   System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |  |
| **Interfejsy, Dysk, Zasilanie** | 1. System realizujący funkcję Firewall musi dysponować minimum: 10 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 4. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB.   System musi być wyposażony w zasilanie AC. |  |
| **Parametry wydajnościowe:** | 1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 750 Mbps.   Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 650 Mbps. |  |
| **Funkcje Systemu Bezpieczeństwa:** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów: SMTP, POP3 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL.   Analiza ruchu szyfrowanego protokołem SSH |  |
| **Polityki, Firewall** | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: 3. Translację jeden do jeden oraz jeden do wielu 4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 5. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 6. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.   Amazon Web Services (AWS).  Microsoft Azure  Cisco ACI.  Google Cloud Platform (GCP).  Nuage Networks VSP.  OpenStack.  VMware vCenter (ESXi).  VMware NSX. |  |
| **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: 2. Wsparcie dla IKE v1 oraz v2. 3. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). 4. Obsługa protokołu Diffie-Hellman grup 19 i 20. 5. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. 6. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. 7. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. 8. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. 9. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. 10. Mechanizm „Split tunneling” dla połączeń Client-to-Site. 11. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: 12. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. 13. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.   Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |  |
| **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie powinno zapewniać obsługę:  Routingu statycznego.  Policy Based Routingu.  Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |  |
| **Zarządzanie pasmem** | System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.  Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.  System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
| **Ochrona przed malware** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |  |
| **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  |
| **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |  |
| **Kontrola WWW** | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |  |
| **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: 2. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. 3. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. 4. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 5. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.   Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |  |
| **Zarządzanie** | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  |
| **Logowanie** | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG |  |
| **Testy wydajnościowe oraz funkcjonalne** | Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta. |  |
| **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy. |  |
| **Gwarancja oraz wsparcie** | System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie .  Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). |  |

1. **Serwer z systemem operacyjnym dla ZWK w Czudcu 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Obudowa** | Typu RACK, wysokość nie więcej niż 1U;  Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable;  Możliwość zainstalowania 8 dysków twardych hot plug 2,5”;  Opcjonalne fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;  Zainstalowane 2 szt. dysków SSD SATA 480 GB Hot-Plug, dyski skonfigurowane 3 x dysków SSD SATA 1,92 TB Hot-Plug podłączone do sprzętowego kontrolera RAID;  Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray |  |
| Płyta główna | Dwuprocesorowa;  Wyprodukowana i zaprojektowana przez producenta serwera;  Możliwość instalacji procesorów 60-rdzeniowych;  Moduł TPM 2.0;  4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5;  Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH;  32 gniazda pamięci RAM;  Obsługa 8 TB pamięci operacyjnej RAM DDR4;  Wsparcie dla technologii:  Memory Scrubbing;  SDDC; ECC;  Memory Mirroring;  ADDDC;  Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.  BIOS UEFI w specyfikacji 2.7. |  |
| **Procesory** | Min jeden procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86\_64;osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 258 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla dowolnego serwera z oferty producenta. |  |
| **Pamięć RAM** | *Min 128 GB pamięci RAM;*  *DDR5 Registered 4800MT/s;* |  |
| Kontrolery LAN | Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:  Min 5x 1G Base-T;  Min 2x 10Gbit SFP+, porty obsadzone modułami SR LC;  Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;  Kontrolery I/O  Kontroler SAS RAID dla dysków wewnętrznych obsługujący RAID 0,1,10 5; |  |
| Porty | Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;  Min 2 porty USB 3.0 dostępne z tyłu serwera;  Min 2 porty USB 3.0 na panelu przednim;  Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;  Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera |  |
| Zasilanie, chłodzenie | Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W; Redundantne wentylatory hotplug |  |
| Zarządzanie | Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;  informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:  karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;  procesory CPU;  pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;  status karty zarządzającej serwera;  wentylatory;  bateria podtrzymująca ustawienia BIOS płyty głównej;  zasilacze;  system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);  Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:  Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;  Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;  Dostęp poprzez przeglądarkę Web, SSH;  Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;  Zarządzanie alarmami (zdarzenia poprzez SNMP);  Możliwość przejęcia konsoli tekstowej;  Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);  Obsługa serwerów proxy (autentykacja);  Obsługa VLAN;  Możliwość konfiguracji parametru Max. Transmission Unit (MTU);  Wsparcie dla protokołu SSDP;  Obsługa protokołów TLS 1.2, SSL v3;  Obsługa protokołu LDAP;  Integracja z HP SIM;  Synchronizacja czasu poprzez protokół NTP;  Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;  Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);  Wbudowana w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;  Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.  Wspierane OS  Microsoft Windows Server 2022, 2019;  VMWare vSphere 8.0;;  Suse Linux Enterprise Server 15;  Red Hat Enterprise Linux 9, 8;  Microsoft Hyper-V Server 2019 |  |
| Gwarancja | Min 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.  Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu;  Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;  Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;  Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty). |  |
| Dokumentacja, inne | Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;  Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;  Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;  W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;  Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;  Należy dostarczyć i wstępnie skonfigurować system zarządzania infrastrukturą IT. Musi być możliwość monitorowania stanu środowiska IT minimum dla oferowanego serwerów. System zarządzania posiada jeden spójny interfejs GUI HTML do zarządzania całym oferowanym środowiskiem sprzętowym. System zarządzania opiera się o tzw. Virtual Appliance kompatybilny z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM. System zarządzania umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe. System zarządzania posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI. System zarządzania musi mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV.  Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;  Serwer musi być certyfikowany do pracy z systemem Ubuntu 22.04;  Zgodność z normami: CB, RoHS, WEEE, GS oraz CE |  |
| **Oprogramowanie** | 1. Licencja na serwerowy system operacyjny Windows SVR 2025 lub oprogramowanie równoważne - system musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie czterech instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Licencja musi w pełni pokrywać licencyjnie rdzenie fizyczne zaproponowanego serwera oraz liczbę użytkowników w ilości min 10 szt.   Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.   1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania  7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:    1. pozwalają na zmianę rozmiaru w czasie pracy systemu,    2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,    3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,    4. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:     1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,     2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o:     1. Login i hasło,     2. Karty z certyfikatami (smartcard),     3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:     1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,     2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:   Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.   * 1. Zdalna dystrybucja oprogramowania na stacje robocze.   2. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej   3. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:   Dystrybucję certyfikatów poprzez http  Konsolidację CA dla wielu lasów domeny,  Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.   * 1. Szyfrowanie plików i folderów.   2. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).   3. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.   4. Serwis udostępniania stron WWW.   5. Wsparcie dla protokołu IP w wersji 6 (IPv6),   6. Wsparcie dla algorytmów Suite B (RFC 4869),   7. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,   8. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:   Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  Obsługi ramek typu jumbo frames dla maszyn wirtualnych.  Obsługi 4-KB sektorów dysków  Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra  Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.  Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)   1. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 2. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 4. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 5. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.   Zorganizowany system szkoleń i materiały edukacyjne w języku polskim |  |

1. **Zakup usługi konfiguracyjnej pozwalającej wdrożyć nowe rozwiązania informatyczne.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (zakres usługi)** | **Potwierdzenie zaoferowania usługi** |
| ***1*** | ***2*** | ***3*** |
| **Usługakonfiguracyjna** | 1. Ogólne wymagania dotyczące instalacji i wdrożenia infrastruktury IT  Wykonawca jest zobowiązany do kompleksowej realizacji procesu instalacji, konfiguracji i uruchomienia dostarczonych urządzeń, gwarantując ich prawidłową integrację z infrastrukturą Zamawiającego. Wszystkie urządzenia muszą zostać wniesione, ustawione oraz zamontowane w szafach teleinformatycznych, a te, które nie są przeznaczone do montażu w szafach rack, powinny być dostarczone do wskazanego miejsca, zamontowane, skonfigurowane i uruchomione. Po zakończeniu prac instalacyjnych wykonawca jest zobowiązany do usunięcia wszelkich opakowań oraz zbędnych materiałów.  Wszystkie dostarczone elementy infrastruktury muszą zostać podłączone do infrastruktury Zamawiającego i skonfigurowane zgodnie z jego wymaganiami. Firmware wszystkich urządzeń musi zostać zaktualizowany do najnowszej stabilnej wersji oferowanej przez producenta. Wykonawca wykona niezbędne połączenia kablowe, uwzględniając dostarczenie i zastosowanie odpowiednich przewodów dla zapewnienia prawidłowej komunikacji oraz podłączenia do zasilania.  2. Konfiguracja oprogramowania SIEM  Wykonawca musi posiadać kompetencje w zakresie projektowania i wdrażania systemów informatycznych, potwierdzone certyfikatami ISO 9001 oraz 27001 lub inne równoważne.  Norma ISO 9001 zawiera szczegółowe wymagania dotyczące systemu zarządzania jakością. Posiadanie ww. certyfikatu zwiększają zdolność firmy do konsekwentnego dostarczania produktów i usług, które spełniają wymagania klientów oraz ustawowe i wykonawcze.  Norma ISO 27001 – System Zarządzania Bezpieczeństwem Informacji, z kolei to międzynarodowy standard określający wymagania dotyczące Systemu Zarządzania Bezpieczeństwem Informacji. Wskazana norma skoncentrowana jest na identyfikacji, zarządzaniu i minimalizowaniu ryzyka związanego z bezpieczeństwem informacji. Obejmuje zarówno aspekty techniczne, organizacyjne, jak i proceduralne.  Poprzez zwrot „równoważny”  Zamawiający rozumie dokument wystawiony przez uprawniony niezależny podmiot, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego.  Zamawiający żąda złożenia dowodu potwierdzającego posiadanie certyfikatu ISO 9001 oraz 2700 lub równoważnych wraz z ofertą na potwierdzenie zgodności oferowanej usługi z wymaganiami określonymi w SZOPZ.  2. Konfiguracja oprogramowania SIEM  W ramach konfiguracji systemu SIEM wykonawca przygotuje infrastrukturę serwerową do wdrożenia systemu, zainstaluje niezbędne systemy operacyjne oraz oprogramowanie na maszynach wirtualnych. Następnie przeprowadzi konfigurację środowiska zgodnie z wymaganiami Zamawiającego, w tym przygotuje pakiety do automatycznej instalacji agentów systemu SIEM na urządzeniach końcowych.  Wykonawca skonfiguruje mechanizmy monitorowania oraz korelacji zdarzeń zgodnie z politykami bezpieczeństwa Zamawiającego, w tym alerty i powiadomienia, raportowanie incydentów oraz analizę logów. System zostanie dostosowany do architektury sieciowej Zamawiającego oraz zintegrowany z pozostałymi elementami środowiska informatycznego.  3. Konfiguracja urządzenia UTM  Urządzenie UTM zostanie skonfigurowane w zakresie adresacji IP zgodnej z architekturą sieciową Zamawiającego. Wykonawca wdroży polityki bezpieczeństwa obejmujące kontrolę ruchu sieciowego, filtrowanie treści oraz mechanizmy zapobiegania zagrożeniom (IPS/IDS).  Zostaną opracowane i wdrożone polityki zdalnego dostępu, w tym konfiguracja klientów VPN dla użytkowników. Wykonawca zapewni również integrację urządzenia UTM z systemem SIEM w celu monitorowania ruchu oraz analizy incydentów bezpieczeństwa.  4. Konfiguracja serwerów  Wykonawca przeprowadzi pełną instalację i konfigurację serwerów, obejmującą uruchomienie systemu operacyjnego, konfigurację macierzy RAID oraz wdrożenie mechanizmów wysokiej dostępności.  Zainstalowane zostaną niezbędne poprawki systemowe, a także zwirtualizowane środowisko serwerowe, w tym usługi Active Directory. Wykonawca skonfiguruje i przetestuje mechanizmy kopii zapasowych oraz wdroży polityki zabezpieczeń na poziomie systemu operacyjnego i warstwy aplikacyjnej.  Przeprowadzone zostaną testy bezpieczeństwa, w tym testy odzyskiwania systemu w przypadku awarii. Wszystkie ustawienia konfiguracyjne zostaną dostosowane do polityki bezpieczeństwa Zamawiającego.  5. Konfiguracja macierzy NAS  W ramach wdrożenia systemu przechowywania danych wykonawca skonfiguruje polityki bezpieczeństwa i dostępu do zasobów przechowywanych na macierzy NAS.  Zostaną wdrożone mechanizmy automatycznych kopii zapasowych oraz polityki retencji danych, zgodnie z wymaganiami Zamawiającego. Wykonawca zapewni pełną integrację systemu NAS z infrastrukturą sieciową oraz usługami katalogowymi, takimi jak Active Directory.  6. Konfiguracja przełączników sieciowych  W ramach wdrożenia infrastruktury sieciowej wykonawca skonfiguruje przełączniki warstwy 2, zapewniając prawidłową segmentację ruchu przy użyciu VLAN-ów.  Adresacja IP zostanie dostosowana do architektury sieciowej Zamawiającego, a polityki bezpieczeństwa na poziomie sieci zostaną wdrożone zgodnie z wymaganiami dotyczącymi izolacji ruchu. Wykonawca skonfiguruje porty przełączników, uwzględniając priorytetyzację ruchu oraz mechanizmy QoS, a także wdroży mechanizmy zabezpieczeń portów, takie jak 802.1X oraz ograniczenia MAC.  7. Instalacja i konfiguracja systemu antywirusowego  Wykonawca zobowiązany jest do wdrożenia w ramach budowanego środowiska również funkcjonującego systemu antywirusowego z centralną konsolą zarządzania.  Wykonawca przeprowadzi testy wydajności i stabilności sieci, sprawdzając poprawność konfiguracji i jej zgodność z wymaganiami Zamawiającego. | ***TAK/NIE\**** |

***\*Wybrać odpowiednie.***

**CZĘŚĆ DEDYKOWANA DLA ZADANIA NR 2: Zadanie nr 2: Dostawa i instalacja agregatów prądotwórczych**

**I. Uwagi ogólne:**

Niniejszy dokument prócz zdefiniowania minimalnych wymagań dotyczących przedmiotu zamówienia, będzie również pełnił funkcje przedmiotowego środka dowodowego w rozumieniu ustawy Pzp. W związku z powyższym Wykonawca zobowiązany jest do dokonania szczegółowej analizy załącznika pod kątem sformułowanych wymogów i wypełnienie stosownych kolumn tabel ujętych w części II i III załącznika. Następnie Wykonawca zobowiązany jest do dołączenia wypełnionego dokumentu do złożonej oferty.

W części II Wykonawca zobowiązany jest do podania oferowanego modelu lub wersji oraz producenta oferowanego asortymentu (w kolumnie 3).

W części III natomiast Wykonawca zobowiązany jest do odniesienia się do opisanego wymogu i wpisanie danych (w kolumnie 3), które będą miały za zadanie jednoznaczne potwierdzenie spełnienie danego wymogu. Wpisy ogólne typu: „zgodne z SWZ” nie będą traktowane przez Zamawiającego jako prawidłowe.

**II. Zestawienie Oferowanego sprzętu, oprogramowania lub usług:**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Przedmiot zamówienia** | **Producent/ Model/Wersja** |
| *1* | *2* | *3* |
| **1.** | **Dostawa awaryjnego źródła zasilania w postaci Agregatu prądotwórczego- centrum zapasowe dla jednostek podległych** |  |
| **2.** | **Dostawa awaryjnego źródła zasilania w postaci Agregatu prądotwórczego dla Urzędu Gminy w Czudcu.** |  |

**III. PARAMETRY SPRZĘTU I UŁUG**

* 1. **Dostawa Awaryjnego źródła zasilania w postaci Agregatu prądotwórczego- centrum zapasowe dla jednostek podległych**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Osadzenie agregatu** | Urządzenie na platformie jezdnej, na przygotowanym do tego terenie |  |
| **Produkcja** | agregat fabrycznie nowy rok produkcji 2024r lub nowszy |  |
| **Moc (zgodnie z ISO8528):** | Praca nominalna P.R.P ­- nie mniej niż 85 kVA / 68 kW  Praca awaryjna L.T. P. – nie więcej niż 78 kVA / 62 kW |  |
| **Napięcie** | 230/400 V, 50 Hz |  |
| **Prąd znamionowy** | Min 112 A |  |
| **Stopień ochrony prądnicy** | IP23 |  |
| **Wymiary zewnętrzne maksymalne** | MAX 2320 x 1140 x 1770 (długość x szerokość x wysokość) mm bez platformy |  |
| **Min. Wyposażenie** | * Podgrzewacz płynu chłodzącego * Zintegrowany prostownik baterii rozruchowych * Samoczynny start po podaniu sygnału startu * Zintegrowany wyłącznik główny prądnicy * Wyłącznik awaryjny * Pomiar poziomu paliwa w % z odczytem na wyświetlaczu sterownika * Zbiornik paliwa zintegrowany z ramą o pojemności 260 l * Wersja w obudowie wyciszonej, odpornej na warunki atmosferyczne   Dostarczony z płynami eksploatacyjnymi (prócz paliwa) |  |
| **Dane ogólne silnika zespołu prądotwórczego** | * Nominalna prędkość obrotowa: 1500 obr/min * Silnik wysokoprężny, 4 cylindrowy, rzędowy z doładowaniem * MIN Moc 69 kW * Instalacja 12 V DC * Regulator prędkości obrotowej: elektroniczny * Zużycie paliwa max. 18,8 l/h przy 100% obciążenia * Układ paliwowy: wtrysk bezpośredni * Silnik zabezpieczony przed   + Niskim ciśnieniem oleju   + Wysoką temperaturą silnika   + Niskim poziomem paliwa * Pojemność skokowa 4,09 l |  |
| **Dane ogólne prądnicy zespołu prądotwórczego** | * Konstrukcja: Bezszczotkowa, synchroniczna, samowzbudna * Wyprodukowana na terenie UE * Stopień ochrony co najmniej IP23 * Miedziane uzwojenie * Elektroniczny regulator napięcia * **Stabilizacja napięcia: +/- 0,25%**   Klasa izolacji: H |  |
| **Dane ogólne panelu sterowania** | * możliwość sterowania układem SZR * zabezpieczający zespół od awarii elektrycznych, mechanicznych * uruchamiający agregat przy sygnale zdalnego startu * realizujący wszystkie wymagania projektowanego układu SZR * z programowalną logiką PLC * menu i komunikaty w języku polskim * wyposażony w USB * modbus RTU * wyświetlacz wskazujący parametry pracy silnika, prądnicy * obsługa trzech poziomów haseł sterownika * Zegar czasu rzeczywistego zasilany z akumulatora wewnętrznego sterownika * Możliwość podłączenia do 32 dowolnie programowalnych wyjść * Możliwość wysyłania powiadomień o zdarzeniach/ ostrzeżeniach/ alarmach na 10 numerów telefonów. Powiadomienia w języku polskim * ostrzeżenie przypominające o serwisie ustawialne w zależności od daty oraz liczby godzin pracy * pamięć min. 300 zdarzeń z rejestracją wszystkich parametrów wyświetlanych w momencie zdarzenia * Automatyczny start agregatu po przekroczeniu parametrów sieci poza zaprogramowane limity. * Pomiar prądu generatora w trzech fazach * Pomiar napięcia generatora w trzech fazach * Pomiar mocy czynnej, biernej i pozornej * Licznik energii czynnej i biernej generatora * Licznik czasu pracy zespołu * Pomiar napięcia akumulatora * Pomiar poziomu paliwa * Pomiar ciśnienia oleju * Pomiar temperatury bloku silnika * Ochrona generatora (częstotliwość , napięcie ,asymetria, przeciążenie)   Dowolnie ustawialne samoczynne testy okresowe- minimum 10 liczników |  |
| **Gwarancja** | Min. 24 miesiące licząc oda daty protokolarnego odbioru przedmiotu zamówienia |  |

**Wykonawca w ramach ostawy i montażu przygotuje miejsce instalacji agregatu wskazane przez Zamawiającego, utwardzając grunt, przygotowując zabezpieczenie w postaci ogrodzenia uniemożliwiającego dostęp osobą postronnym, Wykona modernizacje instalacji elektrycznej w celu podłączenia i uruchomienia dostarczanego urządzenia oraz wykona projekt w celu zgłoszenia wykonanej instalacji przez Zamawiającego do dostawcy energii elektrycznej.**

* 1. **Zakup awaryjnego źródła zasilania w postaci Agregatu prądotwórczego dla Urzędu Gminy w Czudcu.**

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub wymaganej funkcjonalności** | **Charakterystyka (wymagania minimalne)** | **Opis oferowanej funkcjonalności lub parametru** |
| ***1*** | ***2*** | ***3*** |
| **Osadzenie agregatu** | Urządzenie na platformie jezdnej, na przygotowanym do tego terenie |  |
| **Produkcja** | agregat fabrycznie nowy rok produkcji min. 2024 r. lub nowszy |  |
| **Moc (zgodnie z ISO8528):** | Praca nominalna P.R.P ­- nie mniej niż 55 kVA / 44 kW  Praca awaryjna L.T. P. – nie więcej niż 50 kVA / 40 kW |  |
| **Napięcie** | 230/400 V, 50 Hz |  |
| **Prąd znamionowy** | Min 72 A |  |
| **Stopień ochrony prądnicy** | IP23 |  |
| **Wymiary zewnętrzne maksymalne** | MAX 2300 x 1010 x 1565 (długość x szerokość x wysokość) mm bez platformy z tolerancją +/- 15 mm |  |
| **Min. Wyposażenie** | * Podgrzewacz płynu chłodzącego * Zintegrowany prostownik baterii rozruchowych * Samoczynny start po podaniu sygnału startu * Zintegrowany wyłącznik główny prądnicy * Wyłącznik awaryjny * Pomiar poziomu paliwa w % z odczytem na wyświetlaczu sterownika * Zbiornik paliwa zintegrowany z ramą o pojemności 260 l * Wersja w obudowie wyciszonej, odpornej na warunki atmosferyczne   Dostarczony z płynami eksploatacyjnymi (prócz paliwa) |  |
| **Dane ogólne silnika zespołu prądotwórczego** | * Nominalna prędkość obrotowa: 1500 obr/min * Silnik wysokoprężny, 4 cylindrowy, rzędowy z doładowaniem * MIN Moc 53 kW * Instalacja 12 V DC * Regulator prędkości obrotowej: elektroniczny * Zużycie paliwa max. 11,9 l/h przy 100% obciążenia * Układ paliwowy: wtrysk bezpośredni * Silnik zabezpieczony przed   + Niskim ciśnieniem oleju   + Wysoką temperaturą silnika   + Niskim poziomem paliwa * Pojemność skokowa 2,3 l |  |
| **Dane ogólne prądnicy zespołu prądotwórczego** | * Konstrukcja: Bezszczotkowa, synchroniczna, samowzbudna * Wyprodukowana na terenie UE * Stopień ochrony co najmniej IP23 * Miedziane uzwojenie * Elektroniczny regulator napięcia * **Stabilizacja napięcia: +/- 0,5%**   Klasa izolacji: H |  |
| **Dane ogólne panelu sterowania** | * możliwość sterowania układem SZR * zabezpieczający zespół od awarii elektrycznych, mechanicznych * uruchamiający agregat przy sygnale zdalnego startu * realizujący wszystkie wymagania projektowanego układu SZR * z programowalną logiką PLC * menu i komunikaty w języku polskim * wyposażony w USB * modbus RTU * wyświetlacz wskazujący parametry pracy silnika, prądnicy * obsługa trzech poziomów haseł sterownika * Zegar czasu rzeczywistego zasilany z akumulatora wewnętrznego sterownika * Możliwość podłączenia do 32 dowolnie programowalnych wyjść * Możliwość wysyłania powiadomień o zdarzeniach/ ostrzeżeniach/ alarmach na 10 numerów telefonów. Powiadomienia w języku polskim * ostrzeżenie przypominające o serwisie ustawialne w zależności od daty oraz liczby godzin pracy * pamięć min. 300 zdarzeń z rejestracją wszystkich parametrów wyświetlanych w momencie zdarzenia * Automatyczny start agregatu po przekroczeniu parametrów sieci poza zaprogramowane limity. * Pomiar prądu generatora w trzech fazach * Pomiar napięcia generatora w trzech fazach * Pomiar mocy czynnej, biernej i pozornej * Licznik energii czynnej i biernej generatora * Licznik czasu pracy zespołu * Pomiar napięcia akumulatora * Pomiar poziomu paliwa * Pomiar ciśnienia oleju * Pomiar temperatury bloku silnika * Ochrona generatora (częstotliwość , napięcie ,asymetria, przeciążenie) * Dowolnie ustawialne samoczynne testy okresowe- minimum 10 liczników |  |
| **Gwarancja** | Min. 24 miesiące licząc oda daty protokolarnego odbioru przedmiotu zamówienia |  |

**Wykonawca w ramach ostawy i montażu przygotuje miejsce instalacji agregatu wskazane przez Zamawiającego, utwardzając grunt, przygotowując zabezpieczenie w postaci ogrodzenia uniemożliwiającego dostęp osobą postronnym, Wykona modernizacje instalacji elektrycznej w celu podłączenia i uruchomienia dostarczanego urządzenia oraz wykona projekt w celu zgłoszenia wykonanej instalacji przez Zamawiającego do dostawcy energii elektrycznej.**