**Załącznik nr 1 do SWZ**

**Zam. 255/2023/PN/DZP**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

***CZEŚĆ I***

**Pozycja nr 1**

Klaster serwerów proxy.

Klaster co najmniej 2 urządzeń fizycznych działajłących w trybie High Availibilty – 1 zestaw

**Przeznaczenie:**

System podziału obciążenia dla ruchu przychodzącego i wychodzącego pracujący w warstwach sieci 2, 4, 7. Musi zostać dostarczony w postaci komercyjnej platformy sprzętowej lub programowej. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

**Architektura systemu:**

1. Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest, aby system pracował w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa.

2. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe oraz zastosowane w nich technologie, w tym system operacyjny i sprzęt pochodziły od jednego producenta. Nie dopuszcza się, aby elementy funkcji podstawowych zastosowane w systemie były opracowane przez firmy trzecie.

3. Powinna istnieć możliwość implementacji systemu w trybach: one-arm, reverse proxy, transparent proxy.

4. W zakresie sieciowym wymagana jest obsługa IEEE 802.3ad link aggregation.

5. Produkt nie powinien posiadać ograniczeń co do ilości obsługiwanych serwerów.

6. Powinna istnieć możliwość zdefiniowania co najmniej 4 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu.

**Wymagane mechanizmy High Availability**

1. System musi mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive oraz Active-Active.

2. Klastrowanie N+1 bazujące na Stateful session failover zarówno w trybie Active-Passive jak i Active-Active.

3. Synchronizacja konfiguracji pomiędzy elementami klastra w czasie rzeczywistym.

4. Pływające adresy IP oraz grupy dla Stateful failover. Failover jest anonsowany dla sąsiednich urządzeń sieciowych używając Gratuitous ARP.

5. Wbudowane mechanizmy decyzji o failover w oparciu o: reboot systemu, niedostępność interfejsów, brak komunikacji Heartbeat, brak dostępności adresu IP.

6. Synchronizacja konfiguracji po przeładowaniu urządzenia jak i w czasie pracy.

**Parametry fizyczne pojedynczego systemu**

1. System realizujący funkcje podstawowe musi dysponować minimum:

 • 4 portami Gigabit Ethernet RJ-45.

 • 4 gniazdami SFP 1 Gbps.

2. Wbudowany port konsoli szeregowej.

3. Powierzchnia dyskowa - minimum 128 GB.

4. Zasilanie z sieci 230V/50Hz.

5. Obudowa urządzenia o wysokości do 1 U z możliwością montażu w standardowej szafie teletechnicznej 19 cali.

**Parametry wydajnościowe pojedynczego systemu**

1. Przepływność: nie mniej 8 Gbps w warstwie 4 i nie mniej niż 4 Gbps w warstwie 7.

2. Ilość transakcji HTTP na sekundę przy balansowaniu w warstwie 4 – nie mniej niż 1 mln.

3. Ilość nowych połączeń SSL (długość klucza 2048) na sekundę w warstwie 7 (gdzie 1 połączenie obsługuje jedno żądanie http) – nie mniej niż: 4000.

4. Przepływność ruchu poddanego kompresji – nie mniej niż: 5 Gbps.

**Podstawowe funkcje systemu**

System musi realizować co najmniej poniższe funkcje:

1. Podział obciążenia (loadbalancing) dla protokołów:

• dns

• ftp

• http

• https

• ip

• mysql

• DIAMETER

• radius

• rdp

• rtmp

• rtsp

• sip

• smtp

• tcp

• udp

2. Mechanizmamy podziału obciążenia:

• Round Robin,

• Weighted Round Robin,

• Least Connection,

• Fastest Response

3. Wsparcie dla mechanizmów server persistence:

• Source-IP

• Source-IP Hash

• Source-IP/Port Hash

• Hash Header

• Hash Request

• Persistent Cookie

• Rewrite Cookie

• Insert Cookie

• Hash Cookie

• Embedded Cookie

• RADIUS Attribute

• SSL Session ID

• RDP Cookie

4. Weryfikacja stanu pracy serwerów, co najmniej w oparciu o protokoły:

• dns

• ftp

• http

• https

• icmp

• imap4

• l2-detection

• mysql

• DIAMETER

• pop3

• radacct

• radius

• rtsp

• sip

• sip-tcp

• smtp

• snmp

• snmp-custom

• ssh

• tcp

• tcp-echo

• tcphalf

• tcpssl

• udp

• LDAP

• Oracle

5. Możliwość kontroli ruchu produkcyjnego przy uruchamianiu serwerów (warm up rate limiting) oraz przy ich konserwacji (session ramp down).

6. Content routing.

7. Funkcja podmiany zawartości - content rewriting.

8. Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For”.

9. Obsługa języków skryptowych, umożliwiających manipulowanie żądaniami i odpowiedziami w transakcjach, z funkcją debugowania działania skryptów.

10. Podział obciążenia pomiędzy kilka łączy z funkcjami: health check oraz persistence, przy zastosowaniu metod rozkładania ruchu

11. Wyjściowy multi-homing Link Load Balancing używając funkcji virtual tunnel (enkapsulacja GRE) przy wielu łączach wychodzących przy zastosowaniu metod rozkładania obciążenia

12. Load balancing serwerów pomiędzy różnymi data center.

13. Global Load ballancing w oparciu o protokół DNS.

14. Obsługa DNSSEC z możliwością definiowania list kontroli dostępu.

15. Możliwość zdefiniowania co najmniej X interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.

16. W zakresie routingu rozwiązanie powinno zapewniać obsługę protokołów dynamicznego routingu: OSPF oraz BGP.

17. System musi wspierać IPv4 oraz IPv6

**Wymagane funkcje w zakresie SSL-offload:**

1. Obsługa SSL Forward Proxy.

2. Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

3. Bezpieczne dostarczanie aplikacji przy wsparciu szyfrowania SSL.

4. Wparcie formatów certyfikatów: .cer, .pem, and .pfx (PKCS12).

5. Backup i odtwarzanie certyfikatów oraz kluczy prywatnych na dysk lokalny za pośrednictwem interfejsu GUI.

6. Wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej.

7. Możliwość generowania CSR (Certificate Signing Request), self-signed Certificate oraz klucza prywatnego dla określonego hosta.

8. Możliwość dostosowania komunikatów błędów dla zdarzeń SSL.

9. Przepisywanie nagłówka HTTP do HTTPS Host, Request URL, Referer oraz jego manipulację za pomocą skryptów.

10. Wsparcie SSL end-to-end, jako SSL Server i/lub jako SSL Client.

11. Weryfikacja certyfikatu klienta, CRL (HTTP, FTP, LDAP) przez http, SCEP oraz OSCP.

12. Wspierane algorytmy, co najmniej: Elliptic Curve Diffie-Helman, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA384, ECDHE-RSA-AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES128-SHA, ECDHE-RSA-RC4-SHA, ECDHE-RSA-DES-CBC3-SHA.

13. Wsparcie rozszerzeń TLS SNI w połączeniach: client <-> ADC oraz ADC <-> server.

14. Wspiercie wersji SSL/TLS dla serwerów wirtualnych oraz rzeczywistych: TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3.

**Wymagane funkcje w zakresie akceleracji aplikacji:**

1. Optymalizacja wydajności przy użyciu TCP connection multiplexing oraz TCP buffering.

2. Obsługa w czasie rzeczywistym tzw. Dynamic Web Content Compression w celu redukcji obciążenia serwerów z opcją wyboru typu kontentu oraz URI.

3. Selektywna kompresja dla typów MIME, co najmniej: Text, HTML, XML, Java Scripts, CSS, Custom (images).

4. Zaawansowany i wydajny Web cache bazujący na pamięci RAM.

5. W zakresie HTTP cache'owanie obiektów statycznych oraz dynamicznych.

6. Konfiguracja reguł w oparciu, o które działa cache. Powinny one uwzględniać co najmniej: max object size, TTL objects, refresh time interval.

7. Statystyki dostępu do cache bazujące na IP lub http hosts.

8. Obsługa Rate shaping oraz QoS dla: źródła, przeznaczenia i usług.

**Wymagane funkcje w zakresie bezpieczeństwa aplikacji:**

1. Ochrona przed atakami SYN flood oraz SYN Cookie.

2. Stateful firewall dla IPv4 oraz IPv6.

3. Funkcje Web Application Firewall z analizą w oparciu o sygnatury ochrony aplikacji web dostarczane przez producenta rozwiązania i aktualizowane zgodnie z harmonogramem. Mechanizmy analizy i ochrony dla: XSS/SQL injection, HTTP protocol constraints, URL protection, wykrywanie botów, ochrona przed atakami typu Brute force

4. HTTP authentication.

5. Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania.

6. Wsparcie Geo-IP dla ochrony przed DDoS.

7. Limitowanie połączeń w oparciu o polityki.

8. Pełna obsługa OWASP top 10

9. Ochrona przed podmianą strony WWW realizowana bezpośrednio na systemie podziału obciążenia lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcjonalność.

10. Skaner aplikacji WWW realizowany bezpośrednio na systemie podziału obciążenia lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcjonalności.

11. Wsparcie dla walidacji OpenAPI, JSON i XML.

**Wymagane funkcje dodatkowe**

1. Uwierzytelnianie użytkowników w oparciu o: lokalną bazę, LDAP, RADIUS, Kerberos, SAML 2.0.

2. Możliwość uruchomienia ADFSProxy oraz stworzenia polityki w celu sprawdzania ruchu do serwerów ADFS, ich ochrony pod kątem malware, botów, exploitów, oraz ataków DoS, APT i zero day

3. Możliwość przełączenia systemu w tryb inspekcji SSL, z możliwością uruchomienia kategoryzacji filtrowanych stron internetowych

**Zarządzanie**

1. Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, SNMP v1, v2c, v3.

2. Musi dostarczać w GUI informacji o zalogowanych administratorach.

3. Możliwość aktualizacji oprogramowania, backupu i odtwarzania konfiguracji z poziomu GUI.

4. Wsparcie dla REST API do integracji z innymi produktami.

5. Wbudowane narządzie pozwalające na podgląd komunikacji sieciowej, np. Packet Capture.

6. System musi posiadać co najmniej dwie partycje, na których przechowywane jest oprogramowania i konfiguracja.

**Logowanie i Raportowanie**

1. System musi zapewniać lokalne logowanie oraz raportowanie.

2. Możliwość logowania do wielu zewnętrznych serwerów syslog z możliwością określenia facility.

3. Obsługa powiadomień o zdarzeniach systemowych mailem.

4. Powiadomienia o zdarzeniach systemowych za pośrednictwem trapów SNMP, w tym co najmniej zużycie: CPU, RAM, Dysku.

**Sygnatury, subskrypcje**

1. Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie aktualizowane zgodnie ze zdefiniowanych harmonogramem.

2. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:

• Sygnatury ochrony dla aplikacji www, bazy reputacyjne adresów IP na okres minimum 12 miesięcy.

• Sygnatury ochrony dla aplikacji www na okres minimum 12 miesięcy.

• Bazy reputacyjne adresów IP na okres minimum 12 miesięcy.

**Zadania związane z dostawą:**

- instalacja urządzeń w szafie rack Zamawiającego,

- podłączenie urządzeń do infrastruktury Zamawiającego,

- uruchomienie urządzenia i wstępna konfiguracja

- przeszkolenie 2 pracowników Zamawiającego w wymiarze 8 godzin w zakresie obsługi

**Gwarancja oraz wsparcie**

1. System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 12 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 techniczne w trybie 24x7.

**Pozycja nr 2**

Serwery do obsługi baz danych

Klaster serwerów przeznaczonych do obsługi baz danych MS SQL, PostgreSQL, Oracle składający się z 2szt. identycznych serwerów (1 zestaw), które będą dołączone do istniejącego klastra wirtualizacji vMware vSphere wraz systemem zarządzania bazą Active Directory (AD).

Wymagania dotyczące systemu zarządzania AD:

Funkcjonalności aplikacji

możliwość zbiorczego zarządzania użytkownikami Active Directory, a w szczególności:

\* Tworzenie i modyfikację grup Active Directory,

\* Tworzenie kont użytkowników dla wielu użytkowników, w tym unikanie tworzenia duplikatów, poprzez wykorzystywanie dodatkowych elementów w loginie z możliwością podłączenia własnego skryptu, przy tworzeniu nowego użytkownika,

\* Modyfikacja atrybutów dla wielu użytkowników,

\* Reset haseł i odblokowanie kont dla wielu kont użytkowników,

\* Zmianę wyświetlanej nazwy użytkownika,

\* Tworzenie skrzynek mailowych systemu Exchange,

\* Udostępnianie / blokowanie / usuwanie nieaktywnych kont w Active Directory,

\* Przenoszenie użytkowników między jednostkami organizacyjnymi (OU);

możliwość zbiorczego tworzenia nowych użytkowników w Active Directory, a w szczególności:

\* Tworzenie użytkowników przez definiowanie wszystkich atrybutów z uwzględnieniem usług Exchange, Terminal, Lync, Office365,

\* Dodawanie użytkowników przez kopiowanie właściwości innego użytkownika,

\* Import właściwości użytkownika z plików CSV, gdzie jedynym obowiązkowym atrybutem jest nazwa użytkownika,

\* Tworzenie i wykorzystanie szablonów z wspólnymi atrybutami,

\* Tworzenie użytkowników w istniejącym kontenerze lub tworzenie nowej jednostki organizacyjnej (OU) i dodanie do niej użytkowników;

możliwość zbiorczego modyfikowania kont użytkowników w Active Directory, a w szczególności:

Dla kont ogólnych

\* Reset haseł,

\* Reset haseł dla wielu kont,

\* Ustawianie haseł nigdy nie wygasających,

\* Ustawianie haseł, których użytkownik nie może zmienić,

\* Ustawianie haseł, które użytkownik ma obowiązek zmienić przy następnym logowaniu,

\* Usuwanie i blokowanie użytkowników, jeżeli ich hasło wygasło,

\* Modyfikację formatów nazwy, nazwy wyświetlanej, nazwy logowania i nazwy kont SAM (Security Account Manager),

\* Udostępnianie / blokowanie użytkowników, odblokowywanie użytkowników, definiowanie czasu wygaśnięcia kont,

\* Definiowanie katalogów głównych (Home Folder), profile i ścieżek skryptów dla użytkowników,

\* Aktualizację członkostwa grup i list dystrybucyjnych,

\* Przenoszenie użytkowników do innych kontenerów,

w zakresie szablonu modyfikacji użytkownika możliwość skonfigurowania reguł sprawdzających warunek „nie” oprócz istniejącego warunku „jest”,

Dla kont Exchange

\* Tworzenie skrzynek na serwerze Exchange dla użytkowników,

\* Definiowanie wielkości wiadomości przychodzących i wychodzących oraz innych ograniczeń,

\* Ograniczenie limitów adresatów i adresów przekierowania dla użytkowników,

\* Modyfikację limitów składowania poczty i retencji usuniętych obiektów,

\* Udostępnianie / blokowanie dostępu mobilnego do programu Outlook (również w wersji Web), protokołów IMAP4 i POP3,

Dla kont usług terminalowych

\* Modyfikację katalogu głównego usług terminalowych i ścieżek profilowych dla użytkowników,

\* Modyfikację programów startowych dla użytkowników logujących się z usług terminalowych,

\* Modyfikację czasu trwania sesji, limitu aktywnych sesji, limitu bezczynnych sesji, itd.

\* Udostępnianie / blokowanie parametrów zdalnej kontroli,

możliwość podłączenia własnego skryptu, przy tworzeniu nowego użytkownika;

możliwość zarządzania kontami użytkowników nieaktywnych i zablokowanych, a w szczególności:

\* Wyszukiwanie kont użytkowników lub stacji roboczych nie logowanych przez zdefiniowaną ilość dni,

\* Wyszukiwanie wygasłych i niewykorzystywanych kont Active Directory,

\* Lokalizację nieaktywnych kont użytkowników lub stacji roboczych i blokowanie, usuwanie, przenoszenie lub aktywację tych kont,

\* Prezentację zablokowanych kont, czas ostatniego logowania / wylogowania, rodzaj systemu operacyjnego, itd.

\* Eksport raportów do plików CSV, XLS, XLSX, HTML, PDF i CSVDE;

możliwość zarządzania stacjami roboczymi w Active Directory, a w szczególności:

\* Zbiorcze dodawanie / usuwanie stacji roboczych z grup,

\* Zbiorcze przypisanie ogólnych atrybutów takich jak opis, lokalizacja, itp. do stacji roboczych,

\* Zbiorcze blokowanie / odblokowanie stacji roboczych,

\* Zbiorcze przenoszenie stacji roboczych pomiędzy jednostkami organizacyjnymi (OU) w domenie;

możliwość zarządzania udziałami plików na serwerach plików, a w szczególności:

\* Zbiorcze modyfikowanie uprawnień NTFS do plików/folderów,

\* Zbiorcze usuwanie uprawnień NTFS do plików/folderów,

\* Zbiorcze modyfikowanie uprawnień serwera plików za pośrednictwem pliku CSV,

\* obsługa udostępnionych woluminów klastra poprzez zarządzanie uprawnieniami dostępu do udostępnionych woluminów klastra wraz z ich raportowaniem przy użyciu raportów Zarządzania serwerem plików i NTFS,

\* zarządzanie uprawnieniami dostępu do pamięci masowej Netapp i Isilion i raportowania,

\* System posiada możliwość raportowania dostępu do poszczególnych folderów,

 gotowy zestaw wbudowanych raportów: Raport użytkowników, bezpieczeństwa, logowania, z usługi Exchange, haseł, GPO, stacji roboczych, grup, polis, jednostek organizacyjnych, udziałów NTFS, uprawnień i dostępu do katalogów.

możliwość dodawania własnych atrybutów LDAP z AD, do raportów;

możliwość zarządzania i raportowania Office365:

Raporty: użytkowników, grup, kontaktów, licencji, skrzynek pocztowych, OWA,

Raportowanie ostatniej aktywności użytkownika według usługi i ostatniej aktywności użytkownika według daty,

Zarządzanie: użytkownikami, grupami, kontaktami, licencjami, skrzynkami mailowymi, udostępnionymi skrzynkami mailowymi, kalendarzem,

Zarządzanie kanałami i politykami w Microsoft Teams;

możliwość automatycznego wykonywania krytycznych zadań, jak i zamykanie aktywnych sesji w Office365;

możliwość tworzenia szablonów zarządzania Microsoft 365 – grupy Microsoft, grupy obsługujące dystrybucję / bezpieczną pocztę i dynamiczne grupy dystrybucyjne pojedynczo i zbiorczo ze wszystkimi uprawnieniami;

możliwość wysyłania notyfikacji e-mailowych odnośnie wykonywanych akcji w systemie;

możliwość modyfikacji polityk GPO wraz z ustawianiem poszczególnych parametrów;

możliwość zarządzania zakresem obiektów zasad grupy za pomocą opcji filtrowania zabezpieczeń i filtrowania WMI,

opcje konfiguracji uprawnień GPO (edycja, modyfikowanie zabezpieczeń, odczyt lub usuwanie) dla żądanych użytkowników, grup i komputerów;

możliwość wykonania kopii zapasowej obiektów z Active Directory. Dla modułu „Backup” system posiada funkcję „ElasticSearch” w celu uproszczenia przeszukiwania kopii zapasowych;

możliwość konfiguracji automatyzacji w oparciu o własny raport,

opcja Orkiestracji, czyli budowania sekwencji zadań, które mają następować po sobie automatycznie;

możliwość synchronizacji przyrostowej dla zachodzących zmian w usłudze Active Directory;

możliwość dogodnego wstrzymywania, wznawiania, ponawiania i usuwania działań skonfigurowanych w sekcji opóźnionych zadań zarządzania;

możliwość masowego rozwiązywania żądań przepływu pracy, niezależnie od statusu zgłoszenia;

możliwość przeszukiwania AD oraz przesyłanie wyniku do pliku;

możliwość elastycznej migracji użytkowników między domenami w lesie;

możliwość migracji grup między domenami w lesie;

możliwość tworzenia cyklicznych raportów oraz przesłanie wyników drogą mailową;

możliwość w raportach niestandardowych wyświetlania listy kont użytkowników, które wygasną w ciągu najbliższych N dni, korzystanie z filtra proxyAddress podczas tworzenia niestandardowych raportów;

System musi posiadać raporty dynamiczne grup dystrybucyjnych;

System musi udostępniać różne poziomy dostępu tak, aby możliwa była delegacja zadań do pracowników działu wsparcia IT i innych działów bez konieczności dystrybucji uprawnień administratora, z możliwością ograniczenia zadań do poszczególnych jednostek organizacyjnych

oraz domen, a w szczególności:

\* Reset hasła użytkownika,

\* Odblokowanie konta użytkownika,

\* Dodawanie i usuwanie członków grup,

\* Przenoszenie użytkowników do różnych jednostek organizacyjnych w ramach domeny,

\* Dodawanie i usuwanie stacji roboczych w domenie,

\* Tworzenie kont użytkowników,

\* Tworzenie, usuwanie i modyfikacja atrybutów kont użytkowników;

Wbudowane specjalnie przygotowane API, pozwalające:

\* Utworzyć nowego użytkownika w wybranej domenie,

\* Tworzyć OU,

\* Tworzyć użytkownika, wg. Predefiniowanych w systemie szablonów,

\* Restartować hasło użytkownika,

\* Odblokować/zablokować użytkownika,

\* Usunąć użytkownika,

\* ustawić datę, w której wygaśnie konto użytkownika,

\* Wyszukać konkretnego użytkownika w AD, wraz z możliwością:

wyszukania go przy pomocy tekstu,

wymuszenia synchronizacji z AD, przed podaniem wyników wyszukiwania,

posortowania wyników według wybranej kolumny,

posortowania wyników rosnąco lub malejąco;

System musi pozwalać w integracji HRMS na automatyczne wykrywanie kont użytkowników usuniętych z aplikacji HRMS oraz usuwanie odpowiadających im kont Active Directory,

System musi posiadać integrację HCM: umożliwia to integrację aplikacji z dowolnym rozwiązaniem HRMS/HCM z obsługą API;

Prezentacja danych:

Możliwość przedstawienia podstawowych danych nt. Active Directory na panelu, w tym:

\* ilość wszystkich użytkowników,

\* ilość nieaktywnych użytkowników, w ciągu 30 dni,

\* ilość zablokowanych użytkowników,

\* ilość wyłączonych użytkowników,

\* ilość użytkowników z wygaśniętym hasłem,

\* ilość użytkowników, którzy nigdy się nie zalogowali,

\* ilość użytkowników, którzy zalogowali się w ciągu ostatnich 30 dni,

\* ilość komputerów wszystkich,

\* ilość nieaktywnych komputerów, w ciągu 30 dni,

\* Mieć możliwość reprezentacji danych dla różnych domen,

\* Wyświetlać szczegółowe dane, po przejściu do konkretnego elementu,

\* funkcji AD Explorer na wyświetlanie wartości atrybutów Object GUID dla wszystkich obiektów;

Moduł przepływy pracy [workflow], pozwalający na akceptację danej akcji, zażądanej przez zgłaszającego;

Moduł workflow musi posiadać 3 etapy akceptacji: przegląd - weryfikacja danych, akceptacja, wykonanie;

Moduł workflow musi posiadać możliwość wymuszenia akceptacji oraz przeglądu, przez określoną ilość osób, gdzie maksymalna ilość osób to 5;

Możliwość obsługi wielu domen podczas konfiguracji atrybutu memberOf dla obsługiwanych obiektów w zarządzaniu, workflow oraz automatyzacji;

Cechy systemu;

System musi działać w formie aplikacji Internetowej, umożliwiać podłączenie certyfikatu, w formacie .PFX(PKCS12) oraz Java Keystore, działać na pojedynczej bazie danych PostgreSQL lub MSSQL, na systemach z rodziny Windows;

System musi posiadać wbudowane skrypty, które pozwalają na:

\* backup bazy danych,

\* odtworzenie bazy danych,

\* zmianę bazy danych;

System nie może używać wiecej niż jednego konta do połączenia z domeną;

Aktualizacje aplikacji muszą się dobywać poprzez narzędzie z interfejsem graficznym GUI;

możliwość skonfigurowania działania failover, na podstawie drugiej instancji;

możliwość zmiany portu HTTP/HTTPs z poziomu interfejsu graficznego;

możliwość powiadamiania administratorów, jeśli produkt zostanie wyłączony;

możliwość integracji z PAM360, w celu dynamicznego zarządzania dostępami;

możliwość wykonania skryptu z wybranej ścieżki lub z innej bazy danych jak Oracle oraz MSSQL;

możliwość integrację z ServiceDesk Plus Cloud, Jira i Freshservice w celu wykonywania działań IAM, takich jak onboarding użytkowników, włączanie, wyłączanie, odblokowanie i usuwanie kont użytkowników oraz resetowanie haseł z poziomu konsoli helpdesku;

możliwość konfiguracji protokołu TLS z mechanizmami szyfrowania;

możliwość blokowania użytkownikom lub technikom logowania się do programu po określonej liczbie nieudanych prób logowania;

możliwość włączenia captchy podczas logowania użytkowników systemu;

możliwość ograniczania połączeń przychodzących i wychodzących na podstawie adresów IP lub zakresów adresów IP;

możliwość niestandardowych opcji powiadomień SMS;

możliwość dostosowywania parametrów http i konfiguracji nagłówków żądań http;

możliwość wyboru rodzaju kodowania wiadomości (URL lub Base64) oraz parametry do zakodowania;

możliwość delegowania innych zestawów ról dla każdej grupy organizacyjnej do techników pomocy technicznej;

możliwość zmiany domyślnego hasła wbudowanych kont techników poprzez alerty w produkcie oraz wiadomości e-mail;

prezentacja wyniku bezpieczeństwa systemu obliczanego na podstawie konfiguracji [włączenia] różnych ustawień związanych z bezpieczeństwem [takich jak HTTPS, TFA i LDAP SSL]. Ocena bezpieczeństwa zostanie wyświetlona w produkcie po zalogowaniu oraz w okienku licencji;

system musi posiadać zaktualizowane biblioteki Javascript innych firm do następujących wersji w celu zwiększenia bezpieczeństwa: Boostrap 3.4.1, jQuery UI 1.12.1 oraz Moment 2.29;

System musi posiadać zaktualizowany pakiet Java Runtime Environment (JRE) do wersji ZULU JRE 8.

Wymagania minimalne dla nowych serwerów:

**Obudowa** typu rack, o wysokości maksimum 2U, dostarczona wraz z szynami do szafy rack, umożliwiającymi pełne wysunięcie serwera oraz ramieniem porządkującym ułożenie przewodów. Elementy umożliwiające montaż bez użycia narzędzi.

**Procesor:** zainstalowany minimum jeden procesor w architekturze x86, 64 bitowy, minimum 16 rdzenie, o taktowaniu minimum 2,9GHz, osiągający w teście SPEC CPU2017 Integer Rate Result wynik 260 pkt (wynik osiągnięty dla dwóch procesorów). Wynik SPECrate®2017\_int\_base dla oferowanego modelu serwera z oferowanym typem procesora, musi być opublikowany na stronie https://www.spec.org/cpu2017/results/cpu2017.html; wymagana możliwość rozbudowy o drugi identyczny procesor.

**Płyta główna:** Dwuprocesorowa, możliwość instalacji procesorów czetrdziesto-rdzeniowych;

- Minimum 7 złącz PCI Express generacji 4, w tym minimum 4 złącza fizyczne o prędkości x16; 3 złącza fizyczne o prędkości x8; opcjonalnie możliwość uzyskania 2 złączy o pełnej wysokości;

- Dostępne minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express), nie zajmujące klatek dla dysków hot-plug; Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora lub systemu operacyjnego w slocie M.2 bez zajmowania klatek dyskowych serwera;

- 8 portów SATA do podłączania dysków HDD/SSD;

- Zintegrowany moduł TPM 2.0.

**Pamięć RAM:**

Oferowany model serwera musi obsługiwać pamięć nieulotną (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci);

- Minimum 32 gniazda pamięci RAM na płycie głównej, obsługa minimum 4TB pamięci RAM DDR4; obsługa minimum 12TB + pamięć nieulotna.

- Wsparcie dla technologii zabezpieczania pamięci ECC, Memory Scrubbing, SDDC;

- Wsparcie dla konfiguracji pamięci w trybie „Rank Sparing”, Memory Mirroring;

- Zainstalowane 128GB pamięci RAM typu DDR4 Registered, 3200Mhz w kościach jednego typu;

- Zainstalowane 512GB pamięci RAM typu typu nieulotnego, 3200MHz, która musi współpracować poprawnie z zainstalowaną pamięcią RAM.

**Zainstalowane dyski** (wartości minimalne):

- Możliwość zainstalowania 16 dysków 2,5”, hot-plug;

- zainstalowany napęd DVD-RW;

- zainstalowane 3 dyski SSD SATA 800GB, DWDP min. 10.

- Zainstalowany jeden dysk SSD SATA 240GB (M.2) nie zajmujący wnęk dysków hot-plug na potrzeby uruchamiania wirtualizatora Vmware vSphere w wersji 8 (funkcjonalność wymagana, aby dołączyć serwer do posiadanego przez Zamawiającego środowiska vMware vSphere 7, do servera vCenter Server).

**Kontroler dyskowy I/O:**

- Zainstalowany kontroler SAS 12GB, min 4GB pamięci cache, obsługa RAID 0, 1, 5, 6, 10, 50, 60, obsługa dysków SAS, SATA, PCIE-NVME

- Serwer musi umożliwiać instalację wbudowanego napędu LTO-9 bez konieczności dokupowania elementów innych niż sam napęd LTO-9 oraz kompatybilna karta SAS HBA.

**Kontrolery LAN i SAN:**

- Jedna dwuportowa karta LAN 10Gbit/s RJ-45 na płycie głównej lub dedykowanej karcie typu Flexible LOM, z możliwością wymiany interfejsów na 2x 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

- Jedna dwuportowa karta FCSAN 32Gbit/s obsadzona odpowiednimi wkładkami z portami LC MM.

**Porty:**

- zintegrowana karta graficzna ze złączem VGA dostępnym z przodu i z tyłu serwera;

- minimum 6x USB 3.0, minimum 1 wewnętrzne, minimum 2 dostępne z przodu serwera, minimum 2 z tyłu serwera; Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera;

- 1x rj45 1GBit do karty zarządzającej;

**Zasilanie, chłodzenie:**

- Redundantne dwa zasilacze zgodne ze standardem EPA typu hot-plug, o mocy maksymalnej 900W na 1 zasilacz, sprawność energetyczna 94% (klasa Titanium);

- Nadmiarowe chłodzenie – redundantne wentylatory typu hot-plug;

**Zarządzanie:**

- Wbudowane diody informacyjne informujące o stanie serwera – system przewidywania, rozpoznania 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, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zrządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS płyty głównej, zasilacze.

System diagnostyczny musi działać niezależnie od zewnętrznego zasilania serwera – musi posiadać własne zintegrowane źródło zasilania pozwalające na co najmniej jednokrotną weryfikację stanu podzespołów serwera przy braku zasilania lub uszkodzonych zasilaczach serwera;

- 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 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;

• Dostęp poprzez przeglądarkę Web (także SSL, 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)

• Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych)

• Obsługa VLAN

• Obsługa protokołu LDAP

• Synchronizacja czasu poprzez protokół NTP

• Oprogramowanie zarządzające i diagnostyczne 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 itd.).

• Dedykowana, wbudowana w kartę zarządzającą pamięć flash o pojemności minimum 16 GB

• Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;

• 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 (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji;

• BIOS UEFI min. 2.7

• Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą;

• karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego w systemie producenta serwera). Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do serwera bezpośrednio przez producenta. Funkcjonalność wymagana do uruchomienia zaraz po instalacji serwera bez zakupu dodatkowych licencji – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera;

**Wspierane systemy operacyjne:**

Vmware vSphere 7, 8; Windows Server 2019, 2022; Red Hat Enterprise Linux 8; Suse Linux Enterprise Server 15; Oracle Linux 7;

**System operacyjny** – licencja na vSphere Enterprise Plus 8 na wszystkie dołączone procesory z rocznym wsparciem na poziomie Basic. Licencja jest wymagana, aby dołączyć serwer do posiadanego przez Zamawiającego środowiska vMware vSphere, do servera vCenter Server.

**Zadania związane z dostawą:**

- instalacja urządzeń w szafie rack Zamawiającego,

- podłączenie urządzeń do infrastruktury Zamawiającego,

- uruchomienie urządzenia i konfiguracja systemu zarządzania bazami danych

- uruchomienie i przygotowanie systemów do migracji baz PostgreSQL, Maria DB, MSSQL

Dokumentacja i inne:

- Elementy, z których zbudowane są serwery całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie czasu reakcji i naprawy,

- Serwer musi być fabrycznie nowy,

- Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu (dopuszczony język angielski);

- Dostępność części zamiennych przez 5 lat od momentu zakupu serwera,

- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

- Możliwość skutecznego zgłaszania usterek w trybie całodobowym, 7 dni w tygodniu, również w dni świąteczne. Zgłoszenia muszą być akceptowane przez producenta zarówno drogą e-mail, jak również drogą telefoniczną (ogólnodostępna linia telefoniczna z obsługą w języku polskim, w polskiej strefie numeracyjnej. Nie dopuszcza się numerów o podwyższonej płatności), linia telefoniczna musi być czynna 24 godziny przez 7 dni w tygodniu.

- 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.

Certyfikaty producenta sprzętu:

Certyfikat producenta ISO 9001 w zakresie projektowania, produkcji i serwisu produktów, CE oraz ISO 14001 lub równoważny;

Zgodność z normami UE: RoHS, CE;

Gwarancja obejmująca serwer:

- Minimum 60 miesięcy gwarancji producenta serwera na sprzęt realizowanej w miejscu instalacji serwera z gwarantowanym czasem skutecznej naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD Recovery);

- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych,

- W celu zapewnienia odpowiedniego SLA, jako element odbioru technicznego serwera wymaga się dostarczenia potwierdzenia Producenta serwera o okresie obowiązywania gwarancji, reżimie naprawy oraz odpowiednie dane kontaktowe uprawnionego przedstawiciela Zamawiającego zostały zgłoszone przez Wykonawcę do Producenta serwera celem konfiguracji proaktywnego wsparcia/kontaktu w przypadku wystąpienia usterki. Dane zostaną podane przez Zamawiającego z minimum 14 dniowym wyprzedzeniem przed dniem odbioru sprzętu

- Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera;

- Infolinia producenta serwera w języku polskim (w ofercie należy podać nr telefonu), w czasie obowiązywania gwarancji na sprzęt umożliwiająca po podaniu numeru seryjnego weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci RAM, czasu obowiązywania i typu udzielonej gwarancji.

***CZEŚĆ II***

**Pozycja nr 1**

Switche sieci SAN – 2 sztuki jako 1 zestaw

Nowe switche stanowią rozbudowę posiadanych przełączników Brocade G610 o nowe porty w wyższej prędkości przesyłu danych.

**Ilość portów:**

Łączna ilość aktywnych portów FC – 24 z możliwością rozszerzenia do 64 szt. 32gbit/s portów Fibre Channel. Rozbudowa nie może odbywać się poprzez zakup elementów innych niż moduły SFP/SFP+ i poprzez zakup licencji.

W pełni rozbudowany przełącznik nie może zajmować w szafie RACK więcej niż 1U.

**Przepustowość portu**

Porty uniwersalne o przepustowości 32GB/s, z obsługą przepustowości 8Gbit/s i 16 Gbit/s z automatycznym wyborem przepustowości (auto-sensing), obsługa trybu full-duplex dla wszystkich wspieranych przepustowości.

**Interfejsy optyczne**

Moduły do transmisji światłowodowej z prędkością min. 32Gb/s poprzez kabel światłowodowy wielomodowy (Short-Wavelenght) z interfejsem LC, liczba modułów dostosowana do liczby aktywnych portów, możliwość pracy z prędkością 32Gbit/s

**Inne funkcje i wyposażenie**

1. Obsługa trybów pracy portów FC: D\_Port, E\_port, EX\_port, F\_port, N-Port, AE\_Port,

2. Obsługa funkcji PoD (Ports on Demand) - przydziału licencji dla aktywnych portów FC,

3. Aktywne licencje:

a) Webtools,

b) Zoning,

c) Full Fabric,

4. Możliwość zdalnej aktualizacji firmware’u switcha,

5. Możliwość obsługi funkcjonalności:

a) FabricVision, Trunking, Adaptive Networking, Access Gateway,

6. Dedykowany interfejs RJ-45 min 10/100/1000 Mb/s do zarządzania poprzez sieć Ethernet,

7. Możliwość zarzadzania typu in-band poporzez Fibre Channel,

8. Dedykowany interfejs RJ-45 lub DB9 do zarządzania poprzez interfejs szeregowy, dedykowany port USB umożliwiający upgrade FW i zapis logów,

9. Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia,

10. Zarządzanie poprzez przeglądarkę WWW z obsługą połączeń szyfrowanych min. 128-bit SSL oraz poprzez usługę SSH,

11. Zarządzanie poprzez konsole znakową tzw. CLI,

12. Wsparcie dla protokołu SNMP v.3.

**Typ obudowy**

Wysokość przełącznika 1U w systemie montażu w szafie typu rack 19”.

**Zasilanie/chłodzenie**

1. Redundantne zasilacze z możliwością wymiany na gorąco,

2. Wentylatory nadmiarowe zintegrowane w zasilaczach,

3. Chłodzenie typu „Non Porside Exhaust”.

**Komputer administratora sieci SAN:**

Procesor minimum 10 rdzeni, o taktowaniu bazowym min 3,4GHz, wbudowanym 16-rdzeniowym układem graficznym osiągający w teście CPU PassMark wynik nie mniej niż 21 700 punktów. Wynik dostępny na stronie <https://cpubenchmark.net>.

Wyposażony w pamięć RAM 16GB, dysk SSD 512TB, zasilacz USB-C min 96W.

Porty: min. 3 porty Thunderbolt, HDMI, gniazdo słuchawkowe, podświetlana klawiatura w układzie angielski - międzynarodowy, zintegrowany wyświetlacz 14”. Stacja dokująca zawierająca co najmniej porty: HDMI, USB-C, USB-A, LAN 1Gbit, zasilacz.

Zestaw 2 kluczy Yubikey 5C NFC – podany rodzaj kluczy jest już stosowany w dziale Zamawiającego i zakup kolejnego zestawu stanowi uzupełnienie istniejącego mechanizmu logowania. W przypadku zaoferowania rozwiązania równoważnego, w celu zachowania spójności technologicznej należy dostarczyć dodatkowo 3 podwójne zestawy kluczy. Klucze poza możliwością logowania z kluczem włożonym do portu USB lub zbliżeniowo z technologią NFC, klucze muszą umawiać przechowywanie kluczy GPG, logowania SSH.

**Zadania związane z dostawą:**

Dostawa i montaż w szafie rack Zamawiającego;

Uruchomienie, konfiguracja i podłączenie do sieci zamawiającego.

**Serwis, gwarancja i wsparcie techniczne:**

- min. 12 miesięcy gwarancji producenta przełącznika w trybie naprawy w miejscu instalacji z gwarantowanym czasem skutecznej naprawy przełącznika najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD Fixtime);

- Przełącznik musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie producenta lub Wykonawcy potwierdzające spełnienie wymagań dołączone do oferty,

- Możliwość skutecznego zgłaszania usterek w trybie całodobowym, 7 dni w tygodniu, również w dni świąteczne. Zgłoszenia muszą być akceptowane przez producenta zarówno drogą e-mail, jak również drogą telefoniczną (ogólnodostępna linia telefoniczna z obsługą w języku polskim, w polskiej strefie numeracyjnej. Nie dopuszcza się numerów o podwyższonej płatności), linia telefoniczna musi być czynna 24 godziny przez 7 dni w tygodniu.

- Przełącznik musi umożliwiać konfigurację i uruchomienie dedykowanej funkcji automatycznego powiadomienia serwisu producenta o usterce przez samo urządzenie. Funkcjonalność musi pozwalać na otwarcie zgłoszenia serwisowego w bazie serwisowej producenta zgodnie z wymaganym w specyfikacji poziomem wsparcia technicznego. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do przełącznika bezpośrednio przez producenta.

- W celu zapewnienia odpowiedniego SLA, jako element odbioru technicznego przełączników wymaga się dostarczenia potwierdzenia Producenta przełączników o okresie obowiązywania gwarancji, reżimie naprawy oraz odpowiednie dane kontaktowe uprawnionego przedstawiciela Zamawiającego zostały zgłoszone przez Wykonawcę do Producenta serwera celem konfiguracji proaktywnego wsparcia/kontaktu w przypadku wystąpienia usterki. Dane zostaną podane przez Zamawiającego z minimum 14 dniowym wyprzedzeniem przed dniem odbioru sprzętu);

- Dostępność części zamiennych przez 5 lat od momentu zakupu;

- Wymagana jest bezpłatna dostępność poprawek i aktualizacji Firmware w trakcie obowiązywania gwarancji producenta.

**Pozycja nr 2**

Switche sieci LAN – 4 sztuki jako 1 zestaw

Switche będą stanowić rozbudowę posiadanych przełączników Fujitsu Pswitch 2048P o nowe porty w technologii 10Gbit Base-T.

**Ilość portów:**

- Minimum 48 portów 10GBASE-T (RJ45),

- Minimum 6 portów 40G QSFP+,

- Wszystkie porty 10GE/40GE muszą być aktywne,

- Urządzenie musi obsługiwać kable typu QSFP+ Twinax lub równoważne;

**Parametry wydajnościowe:**

- Wymagana jest prędkość przełączania „wirespeed” dla każdego portu,

- Wymagana jest przepustowość przełączania 720 Gbps (1440 Gbps duplex),

- Wymagany rozmiar tablicy MAC – min. 94000.

**Wymiary:**

- Obudowa musi być przeznaczona do montażu w szafie rack 19”,

- Wysokość urządzenia maksymalnie 1U,

- Dostarczony wraz z szynami do montażu w szafie rack;

**Zgodność z protokołami:**

Przełącznik musi obsługiwać następujące protokoły:

- IPv4 / IPv6

- IEEE 802.1ab LLDP,

- IEEE 802.1p Class of Service,

- IEEE 802.3ad LACP,

- IEEE 802.3x Flow Control.

- IEEE 802.1Qaz Enhanced Transmission Selection (ETS),

- IEEE 802.1Qbb Priority Flow Control (PFC),

- IEEE 802.1q VLAN,

- IEEE 802.1x Port Based Network Access Control,IEEE 802.1d Spanning Tree Protocol,

- IEEE 802.1Qau Congestion Notification,

- IEEE 802.1s Multiple Spanning Tree Protocol,

- IEEE 802.1w Rapid Spanning Tree Protocol;

- Wsparcie dla Data Center Bridging (DCB),

- Wsparcie dla FIP snooping,

- Wsparcie dla Edge Virtual Bridging (EVB),

- Obsługę DCVPN gateway (VXLAN, VTEP, NVE),

- Wsparcie dla Static LAG oraz LACP,

- Obsługę 48 portów w LAG,

- IPv4 - ARP / ICMP / IRDPIPv6 – NDP,

- Routing - Routing Information Protocol (RIP / RIPng),

- OSPF,

- Boarder Gateway Protocol 4 (BGP4),

- Virtual Router Redundancy Protocol (VRRP),

- Equal Cost Multi-Path (ECMP),

- UDP Relay,

- DNS Client and DNS Relay,

- Link-Local Multicast Name Resolution (LLMNR),

- Virtual Routing and Forwarding (VRF),

- Wsparcie dla End Host Mode (Switch musi umożliwiać jednoczesną pracę części portów w trybie „End Host Mode” oraz w trybie „Switching”),

- Wsparcie dla technologii virtual port channel (VPC) lub równoważnej,

**Zarządzanie, zabezpieczenia:**

Urządzenie musi zapewniać:

- Port konsoli CLI,

- Dedykowany port RJ45 100/1000Mbps do zarządzania,

- Port USB,

- Wsparcie dla SSHv2,

- Wsparcie dla NETCONF oraz OVSDB,

- Wsparcie dla protokołów Authentication, authorization, and accounting (AAA),

- Wsparcie dla RADIUS,

- Wsparcie dla SNMP v2c, v3,

- Wsparcie dla Remote monitoring (RMON).

**Zasilanie i chłodzenie**

- Oferowane urządzenia muszą być wyposażone w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej, wymienne w trakcie pracy urządzenia,

- Oferowane urządzenie musi być wyposażone w komplet wentylatorów, wymiennych modułowo, umożliwiających wymianę bez konieczności wyłączania przełącznika,

- Każdy zasilacz i moduł wentylatorów muszą posiadać własną sygnalizację LED wskazującą stan poprawnej pracy i stan usterki,

**Wyposażenie:**

Każdy switch musi być wyposażony w

- Kable zasilające min 2,5m,

- Wkładki QSFP+ 40Gbit – 4 szt.,

- Kable MTP kompatybilne z powyższymi wkładkami, 20m – 2szt.,

- Kable twinax QSFP+ 2m – 2szt.,

**Komputer administratora sieci LAN:**

Procesor minimum 10 rdzeni, o taktowaniu bazowym min 3,4GHz, wbudowanym 16-rdzeniowym układem graficznym osiągający w teście CPU PassMark wynik nie mniej niż 21 700 punktów. Wynik dostępny na stronie <https://cpubenchmark.net>.

Wyposażony w pamięć RAM 32GB, dysk SSD 1TB, kartę LAN 10Gbit Eth.

Porty: min. 4 porty Thunderbolt, HDMI, 2x USB A, klawiatura bezprzewodowa z akumulatorem i czytnikiem linii papilarnych, touchpad obsługujący gesty.

Monitor 2szt: 32”; IPS; jasność 400cd/m2; kontrast statyczny 1200:1; kolory 16,7mln; porty: hdmi x2, usb hub x4, słuchawkowe; redukcja niebieskiego światła; wbudowane głośniki; regulacja wysokości, pochylenia; przewody zasilający hdmi, DP-thunderbolt, uchwyt biurkowy obsługujący z regulacją wysokości, kąta pochylenia, obsługujący oferowane monitory.

Zestaw 2 kluczy Yubikey 5C NFC – podany rodzaj kluczy jest już stosowany w dziale Zamawiającego i zakup kolejnego zestawu stanowi uzupełnienie istniejącego mechanizmu logowania. W przypadku zaoferowania rozwiązania równoważnego, w celu zachowania spójności technologicznej należy dostarczyć dodatkowo 3 podwójne zestawy kluczy. Klucze poza możliwością logowania z kluczem włożonym do portu USB lub zbliżeniowo z technologią NFC, klucze muszą umawiać przechowywanie kluczy GPG, logowania SSH.

**Zadania związane z dostawą:**

- Dostawa i montaż w szafie rack Zamawiającego;

- Uruchomienie, konfiguracja i podłączenie do sieci zamawiającego.

Serwis, gwarancja, wsparcie techniczne:

- min. 60 miesięcy gwarancji producenta przełącznika w trybie naprawy w miejscu instalacji z gwarantowanym czasem skutecznej naprawy przełącznika najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD Fixtime);

- Przełącznik musi być fabrycznie nowy

- Możliwość skutecznego zgłaszania usterek w trybie całodobowym, 7 dni w tygodniu, również w dni świąteczne. Zgłoszenia muszą być akceptowane przez producenta zarówno drogą e-mail, jak również drogą telefoniczną (ogólnodostępna linia telefoniczna z obsługą w języku polskim, w polskiej strefie numeracyjnej. Nie dopuszcza się numerów o podwyższonej płatności), linia telefoniczna musi być czynna 24 godziny przez 7 dni w tygodniu.

- Przełącznik musi umożliwiać konfigurację i uruchomienie dedykowanej funkcji automatycznego powiadomienia serwisu producenta o usterce przez samo urządzenie. Funkcjonalność musi pozwalać na otwarcie zgłoszenia serwisowego w bazie serwisowej producenta zgodnie z wymaganym w specyfikacji poziomem wsparcia technicznego. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do przełącznika bezpośrednio przez producenta.

- W celu zapewnienia odpowiedniego SLA, jako element odbioru technicznego przełączników wymaga się dostarczenia potwierdzenia Producenta przełączników o okresie obowiązywania gwarancji, reżimie naprawy oraz odpowiednie dane kontaktowe uprawnionego przedstawiciela Zamawiającego zostały zgłoszone przez Wykonawcę do Producenta serwera celem konfiguracji proaktywnego wsparcia/kontaktu w przypadku wystąpienia usterki. Dane zostaną podane przez Zamawiającego z minimum 14 dniowym wyprzedzeniem przed dniem odbioru sprzętu);

- Dostępność części zamiennych przez 5 lat od momentu zakupu;

- Wymagana jest bezpłatna dostępność poprawek i aktualizacji Firmware w trakcie obowiązywania gwarancji producenta