

Załącznik nr 1
do Zapytania Ofertowego nr 4/2023 z dnia 27.03.2023 r.

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

w ramach projektu nr POIR.01.01.01-00-0163/22, pt. „FAS Control - system adaptacyjnego sterowania procesem produkcji korpusu wodomierza”.

Zakres realizowanych przez oferenta dostaw obejmować będzie:

- a) infrastrukturę serwerową do badań w zakresie integracji danych,
- b) infrastrukturę sieciową do badań w zakresie przesyłania danych procesowych,
- c) infrastrukturę do badań w zakresie wprowadzania i przetwarzania danych produkcyjnych,
- d) infrastrukturę do badań w zakresie wizualizacji danych procesowych.

- Dostarczany sprzęt i materiały muszą być fabrycznie nowe.
- Jeśli w opisie przedmiotu zamówienia, zawartym w zapytaniu ofertowym lub w załącznikach do zapytania ofertowego, występują nazwy konkretnego producenta/produktu czy normy jakościowe, to należy je traktować jedynie jako pomoc w opisie przedmiotu zamówienia. W każdym przypadku dopuszczalne są rozwiązania równoważne pod względem konstrukcji, materiałów, funkcjonalności, jakości (nie gorsze niż założone w tym załączniku). Użycie takich rozwiązań nie ma wpływu na przyjęcie bądź wykluczenie oferty. Dopuszczenie równoważności dotyczy każdego przypadku użycia nazwy własnej, a nie tylko tam gdzie dodatkowo podkreślono to w specyfikacji.

UWAGA dla pozycji od 1 do 6:

Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie pochodziły od jednego producenta.

1. Routery wraz z konfiguracją – ilość: 2 sztuki

- A. Dostarczone urządzenie NGFW musi zapewniać** wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza:
- i. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
 - ii. W ramach oferty system musi zostać dostarczony w postaci redundantnej.
 - iii. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP.
 - iv. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
 - v. System musi umożliwiać monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych, a także monitoring stanu realizowanych połączeń VPN.
 - vi. Urządzenia powinny posiadać po dwa zasilacze (2xPS)
- B. System realizujący funkcję Firewall musi dysponować minimum:**
- 16 portami Gigabit Ethernet RJ-45,
 - 8 gniazdami SFP 1 Gbps.,
 - 2 gniazdami SFP+ 10Gbps.
- C. Parametry wydajnościowe:**
- i. W zakresie Firewall'a obsługa nie mniej niż 1,5 mln jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę,
 - ii. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B,



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

- iii. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2,1 Gbps.,
- iv. Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.,
- v. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno klient side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix – minimum 2,5 Gbps.,
- vi. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus – minimum 1 Gbps.,
- vii. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

D. Funkcje kontroli bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

- i. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection,
- ii. Kontrola Aplikacji,
- iii. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN,
- iv. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS,
- v. Ochrona przed atakami - Intrusion Prevention System,
- vi. Kontrola stron WWW - Web Threat Protection,
- vii. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3,
- viii. Zarządzanie pasmem (QoS, Traffic shaping),
- ix. Mechanizmy ochrony przed wyciekami poufnej informacji (DLP),
- x. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.
W ramach oferty powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site,
- xi. Analiza ruchu szyfrowanego protokołem SSL,
- xii. Analiza ruchu szyfrowanego protokołem SSH.

E. 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.

- i. Amazon Web Services (AWS),
- ii. Microsoft Azure,
- iii. Cisco ACI,
- iv. Google Cloud Platform (GCP),
- v. OpenStack,
- vi. VMware vCenter (ESXi).

F. Połączenia VPN - System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

- i. Wsparcie dla IKE v1 oraz v2,
- ii. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM),
- iii. Obsługa protokołu Diffie-Hellman grup 19 i 20,
- iv. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE,
- v. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site,
- vi. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności,
- vii. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego,
- viii. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth,
- ix. Mechanizm „Split tunneling” dla połączeń Client-to-Site.



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

G. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

- i. 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.,
- ii. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta,
- iii. Producent rozwiązania musi dostarczać rozwiązanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

H. Ochrona przed atakami:

- i. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych,
- ii. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach,
- iii. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora,
- iv. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur,
- v. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS,
- vi. 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,
- vii. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

I. Kontrola aplikacji:

- i. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- ii. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- iii. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
- iv. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
- v. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

J. Moduły sieciowe:

- i. Każde urządzenie powinno być wyposażone w 2 moduły 10GE SFP+ transceiver module, short range.

K. Zarządzanie:

- i. 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,
- ii. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów,
- iii. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego,
- iv. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow,
- v. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację,



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

- vi. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall,
- vii. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

L. Logowanie:

- i. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania, raportowania, korelacji zdarzeń, powiadamiania o incydentach) udostępnianej w chmurze lub w ramach oferty musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej,
- ii. 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,
- iii. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu,
- iv. Musi istnieć możliwość logowania do serwera SYSLOG.

M. Serwisy:

- i. W ramach postępowania muszą zostać dostarczone rozwiązania upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów.
- ii. Powinny one obejmować kontrolę 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 60 miesięcy.

N. Gwarancja i wsparcie:

Urządzenie musi być objęte serwisem gwarancyjnym przez okres 60 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.

2. Switche (Przełączniki) wraz z konfiguracją – ilość: 12 sztuk**A. Parametry fizyczne platformy:**

- i. Wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U,
- ii. Zasilanie 230V, maksymalny pobór mocy 896W,
- iii. Dostępne zasilanie PoE 740W,
- iv. Zakresy temperatury pracy – 0-45°C,
- v. Zakres temperatury przechowywania – -20-70°C,
- vi. MTBF > 10lat.

B. Interfejsy sieciowe – wymagania minimalne:

- i. 48 porty 1 GE PoE standard 802.3af/at,
- ii. 4 porty 10 GE SFP+ z obsługą wkładek SFP 1GE.

C. Zarządzanie:

- i. Dedykowany interfejs do zarządzania GE – RJ-45,
- ii. Port konsoli szeregowej,
- iii. Zarządzanie przez konsolę szeregową (SSH) oraz poprzez graficzny interfejs oraz poprzez przeglądarkę,



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

- iv. Możliwość zarządzania poprzez kontroler przełączników pozwalający na automatyczne wykrywanie i centralne konfigurowanie przełączników oraz będący jednocześnie konsolą do zarządzania rozwiązaniami NGFW (Next Generation Firewall),
- v. Kontroler przełączników musi być w stanie wykonywać pewne akcje automatycznie, bez ingerencji administratora, a pod wpływem rozpoznanej topologii – m.in. automatyczna konfiguracja Spanning Tree, tagowanie 802.1q, automatyczne przejście zarządzania nad wykrytym przełącznikiem,
- vi. Kontroler przełączników musi umożliwiać aktualizację oprogramowania zarządzanych przełączników,
- vii. Z poziomu kontrolera musi być możliwość podejrzenia informacji o typie urządzeń wykrytych na wybranym porcie przełącznika (np. system Linux, Windows itp.).

D. Parametry wydajnościowe:

- i. Przepustowość urządzenia - min. 176 Gbps, min. 260 Mpps,
- ii. Możliwość zapamiętania co najmniej 32.000 adresów MAC,
- iii. Opóźnienie - poniżej 1 mikrosekund,
- iv. Bufor pakietów: min. 2 MB,
- v. Pamięć DRAM: min. 512 MB DDR3.

E. Wymagane funkcje:

- i. Możliwość automatycznej negocjacji prędkości i duplexu dla połączeń,
- ii. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree), ilość instancji min. 16,
- iii. Możliwość agregacji portów zgodna z 802.3ad, ilość grup min. 16, ilość portów w grupie: min. 8,
- iv. Obsługa co najmniej 4000 VLANów, zgodna z 802.1Q,
 - v. Możliwość wykonywania routingu statycznego,
 - vi. Możliwość wykonywania routingu dynamicznego (OSPFv2, RIPv2),
- vii. Wsparcie dla ECMP (Equal-cost multi-path routing) oraz BFD (Bidirectional Forwarding Detection),
- viii. Funkcjonalność DHCP Relay, DHCP Snooping, Dynamic ARP Inspection, IGMP Snooping,
- ix. Port-mirroring,
- x. Obsługa sFlow,
- xi. Obsługa list kontrolnych ACL, min. 3000 wpisów,
- xii. Wsparcie dla protokołu wysokiej dostępności MCLAG (multi-chassis link aggregation),
- xiii. Kontrola dostępu na poziomie portu w oparciu o standard 802.1x (port oraz MAC-based), możliwość uwierzytelniania w oparciu o bazę Radius,
- xiv. Zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS,
 - xv. Wsparcie dla SNMP, LLDP (w trybie odbioru),
 - xvi. Wsparcie dla SNMP w wersjach 1 – 3,
- xvii. Możliwość zarządzania przez interfejs graficzny i tekstowy,
- xviii. Możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI,
- xix. Wsparcie dla HTTP REST API dla konfiguracji i monitoringu,
- xx. Możliwość integracji z systemem bezpieczeństwa NGFW (Next Generation Firewall) polegającej na przekierowaniu całego ruchu w obrębie tego samego VLAN-u przez urządzenie NGFW i filtracja tego ruchu z wykorzystaniem mechanizmów NGFW, np. IPS, AV,
- xxi. Możliwość integracji z systemem bezpieczeństwa NGFW, w zakresie co najmniej:
 - możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników,
 - obsługa białych i czarnych list MAC,
 - stateful firewall, umożliwiający kontrolę dostępu do sieci.

F. Moduły sieciowe:

Wraz z przełącznikami należy dostarczyć następujące moduły sieciowe:

- i. Każde urządzenie powinno być wyposażone w 2 moduły 10GE SFP+ transceiver module, short range.



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

G. Gwarancja i wsparcie:

Urządzenie musi być objęte serwisem gwarancyjnym przez okres 60 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.

3. Switche światłowodowe wraz z konfiguracją – ilość: 2 sztuki**A. Parametry fizyczne platformy:**

- i. Wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U,
- ii. Redundantne zasilanie 230V, maksymalny pobór mocy 176W,
- iii. Zakresy temperatury pracy – 0-40°C,
- iv. Zakres temperatury przechowywania – -25-70°C,
- v. MTBF > 10lat.
- vi. 2 zasilacze (2xPS)
- vii. kabel łączący 100 GE – 2 szt.

B. Interfejsy sieciowe – wymagania minimalne:

- i. 24 porty 10 GE SFP+ (z obsługą wkładek 1GE),
- ii. 2 portów 40 GE QSFP+/100 GE QSFP+/QSFP28.

C. Zarządzanie:

- i. Dedykowany interfejs do zarządzania GE – RJ-45,
- ii. Port konsoli szeregowej.
- iii. Zarządzanie przez konsolę szeregową (SSH) oraz poprzez graficzny interfejs poprzez przeglądarkę,
- iv. Możliwość zarządzania poprzez kontroler przełączników pozwalający na automatyczne wykrywanie i centralne konfigurowanie przełączników oraz będący jednocześnie konsolą do zarządzania rozwiązaniami NGFW (Next Generation Firewall),
- v. Kontroler przełączników musi być w stanie wykonywać pewne akcje automatycznie, bez ingerencji administratora a pod wpływem rozpoznanej topologii – m.in. automatyczna konfiguracja Spanning Tree, tagowanie 802.1q, automatyczne przejęcie zarządzania nad wykrytym przełącznikiem,
- vi. Kontroler przełączników musi umożliwiać aktualizację oprogramowania zarządzanych przełączników,
- vii. Z poziomu kontrolera musi być możliwość podejrzenia informacji o typie urządzeń wykrytych na wybranym porcie przełącznika (np. system Linux, Windows itp.).
- viii. 2 zasilacze (2xPS)

D. Parametry wydajnościowe:

- i. Przepustowość urządzenia - min. 880 Gbps, min. 1309 Mpps,
- ii. Możliwość zapamiętania co najmniej 64.000 adresów MAC,
- iii. Opóźnienie - poniżej 1 mikrosekund,
- iv. Bufor pakietów: min. 8 MB,
- v. Pamięć DRAM: min. 8 GB.

E. Wymagane funkcje:

- i. Możliwość automatycznej negocjacji prędkości i duplexu dla połączeń,
- ii. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree), ilość instancji min 15,
- iii. Możliwość agregacji portów zgodna z 802.3ad, ilość grup min. 48, ilość portów w grupie: min. 48,
- iv. Obsługa co najmniej 4000 VLANów, zgodna z 802.1Q,
- v. Możliwość wykonywania routingu statycznego,



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

- vi. Możliwość wykonywania routingu dynamicznego (OSPFv2, RIPv2),
- vii. Wsparcie dla ECMP (Equal-cost multi-path routing) oraz BFD (Bidirectional Forwarding Detection),
- viii. Funkcjonalność DHCP Relay, DHCP Snooping, Dynamic ARP Inspection, IGMP Snooping,
- ix. Port-mirroring,
- x. Obsługa sFlow,
- xi. Obsługa list kontrolnych ACL, min. 3000 wpisów,
- xii. Wsparcie dla protokołu wysokiej dostępności MCLAG (multi-chassis link aggregation),
- xiii. Kontrola dostępu na poziomie portu w oparciu o standard 802.1x (port oraz MAC-based), możliwość uwierzytelniania w oparciu o bazę Radius,
- xiv. Zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS,
- xv. Wsparcie dla SNMP, LLDP (w trybie odbioru),
- xvi. Wsparcie dla SNMP w wersjach 1 – 3,
- xvii. Możliwość zarządzania przez interfejs graficzny i tekstowy,
- xviii. Możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI,
- xix. Wsparcie dla HTTP REST API dla konfiguracji i monitoringu,
- xx. Możliwość integracji z systemem bezpieczeństwa NGFW (Next Generation Firewall) polegającej na przekierowaniu całego ruchu w obrębie tego samego VLAN-u przez urządzenie NGFW i filtracja tego ruchu z wykorzystaniem mechanizmów NGFW, np. IPS, AV,
- xxi. Możliwość integracji z systemem bezpieczeństwa NGFW, w zakresie co najmniej:
 - możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników,
 - obsługa białych i czarnych list MAC,
 - stateful firewall, umożliwiający kontrolę dostępu do sieci,
 - routing statyczny i dynamiczny, co najmniej OSPF.

F. Moduły sieciowe:

Wraz z przełącznikami należy dostarczyć następujące moduły sieciowe:

- i. Każde urządzenie powinno być wyposażone w 16 modułów 10GE SFP+ transceiver module, short range.

G. Gwarancja i wsparcie:

Urządzenie musi być objęte serwisem gwarancyjnym przez okres 60 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.

4. AP (Punkty dostępowe) wraz z konfiguracją – ilość: 18 sztuk

- A. Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym za pomocą zintegrowanego kontrolera WiFi dostępnego z interfejsu zarządzania zapory sieciowej (zapora sieciowa powinna mieć wbudowaną funkcjonalność kontrolera sieci bezprzewodowej).
- B. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
 - i. Temperatura 0-50°C,
 - ii. Wilgotność 5–90%.
- C. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington.
- D. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
 - i. 2.4 GHz 802.11b/g/n/ax ze wsparciem dla kanałów 20/40MHz,
 - ii. 5GHz 802.11a/n/ac/ax ze wsparciem dla kanałów 20/40/80MHz,
 - iii. 2.4/5GHz dedykowany skaner spectrum.



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

- E.** Urządzenie musi być wyposażone w moduł radiowy Bluetooth/BLE. Orthogonal Frequency Division Multiple Access (OFDMA)
- F.** Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
- G.** Liczba interfejsów:
- 2x Ethernet w standardzie 10/100/1000 Base-TX,
 - Port szeregowy RS-232 RJ-45,
 - Port USB 2.0.
- H.** Urządzenie powinno być zasilane poprzez minimum jeden interfejs ETH w standardzie 802.3af/at lub zewnętrzny zasilacz.
- I.** Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
- Tunnel,
 - Bridge,
 - Mesh.
- J.** Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
- K.** Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
- DL-MU-MIMO – 2x2, 1x1 w przypadku radia pracującego jako dedykowany skaner
 - Transmit Beam Forming (TxBF),
 - Maksymalna przepustowość dla poszczególnych modułów radiowych:
 - 570 Mbps,
 - 1200 Mbps.
 - Wymagana moc nadawania:
 - min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm,
 - min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm.
 - Wsparcie dla 802.11n 20/40Mhz HT,
 - Anteny – 3 wewnętrzne dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz,
 - Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
 - Maksymalna deklarowana liczba klientów per moduł radiowy – 512.
- L.** Punkt dostępowy musi być certyfikowanym urządzeniem WiFi Alliance oraz posiadać certyfikację DFS.
- M. Gwarancja i wsparcie:**
Urządzenie musi być objęte serwisem gwarancyjnym przez okres 60 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.

5. Urządzenie do dwuetapowego uwierzytelniania wraz z konfiguracją – ilość: 1 sztuka

A. Wymagania ogólne:

System powinien pozwalać na nie mniej niż:

- Graficzną reprezentację statusu uwierzytelnień,
- Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia i nazwy użytkownika:



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

- lokalnie,
- zdalnie w oparciu o protokół syslog.
- iii. Aktualizację systemu operacyjnego z poziomu graficznego interfejsu zarządzającego (GUI),
- iv. Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI),
 - również w oparciu o harmonogram w cyklu godzinowym, dziennym, tygodniowym lub miesięcznym wraz z określeniem godzin i minut,
 - rzezoną kopia bezpieczeństwa może również być również zapisywana przy pomocy protokołu FTP/SFTP,
 - szyfrowanie kopii bezpieczeństwa.
- v. Konfigurację captive portal.

B. Architektura:

Dostarczony system uwierzytelniania musi zapewniać wszystkie wymienione poniżej funkcje. Oferowane rozwiązanie musi pozwalać na centralne zarządzanie kontami użytkowników i ich uwierzytelnianiem.

C. System operacyjny:

Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny, wzmocniony (hardenend) z punktu widzenia bezpieczeństwa.

D. Parametry fizyczne systemu:

- i. System musi zapewniać obsługę nielimitowanej licencyjnie liczby wirtualnych procesorów,
- ii. maksymalnie 1TB pamięci operacyjnej,
- iii. 4 wirtualne interfejsy sieciowe,
- iv. obsługa powierzchni dyskowej - minimum 16 TB.
- v. Możliwość uruchomienia na platformach: Microsoft Hyper-V Server 2010, 2012 R2 oraz 2016, VMware ESXi / ESX 4 / 5 / 5 / 6, KVM, XEN oraz platformach chmury publicznej Microsoft Azure, Amazon AWS, Oracle OCI i AliCloud.

E. Uwierzytelnianie:

Celem realizacji funkcji uwierzytelniających, system powinien wspierać realizację funkcjonalności SSO (Single Sign On) w oparciu o:

- i. Integrację z Active Directory również bez konieczności instalacji dodatkowych rozwiązań na kontrolerach domeny,
- ii. Dedykowaną aplikację na stację robocze z systemem Windows,
- iii. RADIUS,
- iv. Informacje uzyskiwane poprzez protokół syslog,
- v. Dedykowany portal.

F. Wymagania funkcjonalne - uwierzytelnianie dwuskładnikowe:

Realizując uwierzytelnianie dwuskładnikowe, system musi spełniać nie mniej niż:

- i. Obsługę dla tokenów sprzętowych (hardware):
 - ich działanie musi być realizowane w oparciu o protokół OAuth wraz ze wsparciem dla TOTP oraz HOTP,
 - wspomniane tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania.
- ii. Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile (lub równoważnych)
- iii. Dla tokenów na system iOS i Android wymaga się:
 - aktywacji z centralnego systemu uwierzytelniania (seed provisioning),
 - możliwości konfiguracji ilości generowanych cyfr (6 lub 8),
 - generowania kodu (cyfr) co 30 lub 60 sekund,
 - możliwości dezaktywacji tokena oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne),
 - ochrony dostępu poprzez konfigurowalny kod PIN,



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

- aktywacji w oparciu o kod QR,
- możliwość przypisania własnego logotypu organizacji widocznego w aplikacji tokena mobilnego.
- iv. Możliwość dostarczenia kodu (wskazania tokena) poprzez:
 - email (wygaśnięcie kodu w czasie 10-3600 sekund),
 - SMS (wygaśnięcie kodu w czasie 10-3600 sekund):
 - konfiguracja bramki SMS w oparciu o HTTP/S i/lub SMTP.
- v. W przypadku tokenów programowych możliwość wykorzystania notyfikacji push przychodzących na urządzenie mobilne i zawierających szczegóły dotyczące żądania logowania (nazwa użytkownika, serwer/usługa docelowa, adres IP, data i godzina, rodzaj i wersja przeglądarki) w celu zaakceptowania ich jednym "kliknięciem",
- vi. Możliwość integracji z logowaniem do systemu Windows,
- vii. Wsparcie dla API.

G. Wymagania funkcjonalne - 802.1x

System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki:

- i. Dla sieci bezprzewodowych wymagane są następujące protokoły:
 - PEAP,
 - EAP-TTLS,
 - EAP-TLS,
 - EAP-GTC.
- ii. Wsparcie dla uwierzytelniania w oparciu o adres MAC (MAC based authentication),
- iii. Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTL, TLS EAP,
- iv. Możliwość samodzielnej rejestracji urządzeń przez użytkowników celem uwierzytelniania z wykorzystaniem certyfikatów.

H. Wymagania funkcjonalne - zarządzanie certyfikatami:

System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż:

- i. Własne, samodzielne CA (Certificate Authority),
- ii. CA pośredniczące (intermediary CA),
- iii. Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego,
- iv. Możliwość pobrania wygenerowanych certyfikatów,
- v. Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP,
- vi. Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP,
- vii. Możliwość generowania certyfikatów typu wildcard,
- iii. Realizacja CRL (Certificate Revocation List),
- ix. Wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560).

I. Parametry wydajnościowe oraz ilościowe:

Urządzenie musi obsługiwać co najmniej:

- i. Uwierzytelnianie dla 100 użytkowników,
- ii. 25 tokenów (uwierzytelnianie dwuskładnikowe),
- iii. 100 klientów protokołu RADIUS (urządzeń NAS),
- iv. 20 grup,
- v. 10 certyfikatów głównych (CA),
- vi. 100 certyfikatów użytkowników.

J. Gwarancja i wsparcie:

Urządzenie musi być objęte serwisem gwarancyjnym przez okres 60 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.



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

6. Centralny system logowania, raportowania i korelacji, umożliwiający centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach infrastruktury zabezpieczeń wraz z konfiguracją – ilość: 2 sztuki

A. Wymagania Ogólne:

- i. W ramach oferty wymagany jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach infrastruktury zabezpieczeń.
- ii. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy programowej.

B. Parametry wydajnościowe:

System musi być w stanie przyjmować minimum 5GB logów na dzień.

C. Logowanie:

- i. Podgląd logowanych zdarzeń w czasie rzeczywistym,
- ii. Możliwość przeglądania logów historycznych z funkcją filtrowania,
- iii. Możliwość dostosowania widoku wyświetlanych logów poprzez dodawanie, usuwanie oraz zmianę kolejności kolumn zawierających elementy logowanego zdarzenia,
- iv. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia NGFW oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa na przestrzeni zadanego czasu. Muszą one obejmować co najmniej:
 - Listę najczęściej wykrywanych ataków,
 - Listę najbardziej aktywnych użytkowników/źródeł ruchu,
 - Listę najczęściej wykorzystywanych aplikacji,
 - Listę najczęściej odwiedzanych stron www,
 - Listę krajów, do których nawiązywane są połączenia,
 - Listę najczęściej wykorzystywanych polityk Firewall,
 - Informacje o realizowanych połączeniach IPSec i SSL VPN,
 - Listę najczęściej występujących zdarzeń systemowych.
- v. Rozwiązanie musi posiadać możliwość przysyłania kopii logów do innych systemów logowania i przetwarzania danych za pomocą protokołu Syslog i/lub CEF. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów,
- vi. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem portów UDP/514 oraz TCP/514,
- vii. System musi umożliwiać cykliczny eksport logów do zewnętrznego systemu w celu ich długoterminowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP i/lub SCP. Administrator musi mieć możliwość określenia, kiedy ma następować eksport logów,
- viii. System musi prezentować informacje na temat ilości przestrzeni dyskowej wykorzystanej na przechowywanie logów.

D. Raportowanie:

W zakresie raportowania system musi zapewniać:

- i. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV,
- ii. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników,
- iii. Funkcję definiowania własnych raportów,
- iv. Możliwość spolszczenia raportów,



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

- v. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email oraz automatycznego przesłania raportu na zewnętrzny serwer za pomocą protokołu FTP lub SCP,
- vi. Możliwość filtrowania danych uwzględnianych w procesie tworzenia danego raportu, m.in. możliwość ograniczenia zakresu raportu do danych z wybranych urządzeń NGFW a także z wybranej adresacji IP,
- vii. Możliwość automatycznego usuwania raportów po określonym czasie.

E. Korelacja logów:

- i. Możliwość tworzenia własnych reguł korelowania logów,
- ii. Konfigurację powiadomień poprzez: e-mail, SNMP oraz API http w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. W treści powiadomienia musi być możliwość przekazania dodatkowych informacji o zdarzeniu wywołującym dane powiadomienie, np. nazwa wykrytego zagrożenia,
- iii. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
 - Malware/AV,
 - Aplikacje sieciowe,
 - Email,
 - IPS,
 - Web Filter,
 - Traffic (logi z ruchu sieciowego),
 - Systemowe (m.in. utracone połączenie VPN, utracone połączenie sieciowe, zdarzenia związane z klastrem niezawodnościowym, zmiana w sieci SD-WAN).
- iv. Możliwość automatycznego, zwrotnego powiadomienia systemu bezpieczeństwa NGFW o wystąpieniu wybranych zdarzeń korelacji.

F. Zarządzanie:

- i. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów,
- ii. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, Tacacs+, PKI,
- iii. System musi umożliwiać definiowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do wybranych modułów systemu logowania i raportowania,
- iv. System musi mieć możliwość podziału na wirtualne systemy logowania i raportowania (konteksty/domeny). Musi istnieć możliwość przypisywania administratorom praw dostępu do wybranych kontekstów. Dla każdego kontekstu musi być możliwość niezależnego przydzielania zasobów dyskowych oraz określania maksymalnego czasu przechowywania logów.

G. Gwarancja i wsparcie:

Urządzenie musi być objęte serwisem gwarancyjnym przez okres 60 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.



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

7. Serwery wraz z konfiguracją i instalacją oprogramowania

A. Serwer typ 1 – ilość: 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max. 1U wyposażona w komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów 3rd Generacji Intel Xeon.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych
Procesor	Zainstalowane dwa procesory z serii GOLD min. 8-rdzeniowe klasy x86, min. 3.2GHz
RAM	Minimum 512GB DDR4 RDIMM 3200MT/s w modułach min. 32GB, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC
Gniazda PCI	Min. 2 sloty PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe). Dodatkowo zainstalowane: <ul style="list-style-type: none"> 2 interfejsy 10/25GB w standardzie SFP28, wyposażone we wkładki światłowodowe SFP+ 10Gb MM SR, 2 interfejsy FC 16 Gbps.
Dyski twarde	Zainstalowane 2 dyski M.2 SATA o pojemności min. 240GB Hot-Plug w konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Wbudowane porty	Min. 3 porty USB, w tym min. 1 port USB 3.0 Min. 2 porty VGA, Możliwość rozbudowy o Serial Port
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 800W każdy.
System operacyjny/dodatkowe oprogramowanie	Microsoft Windows Server 2022 Datacenter (lub równoważny)



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

Bezpieczeństwo	<ul style="list-style-type: none"> • Blokada służąca do ochrony nieautoryzowanego dostępu do dysków twardych, • Możliwość wyłączenia w BIOS funkcji przycisku zasilania, • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła, • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą, • Moduł TPM 2.0, • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera, • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.
Diagnostyka	<p>Serwer wyposażony w panel LCD umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.</p>
Karta Zarządzania	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:</p> <ul style="list-style-type: none"> • Zdalny dostęp do graficznego interfejsu Web karty zarządzającej, • Zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera), • Szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika, • Możliwość podmontowania zdalnych wirtualnych napędów, • Wirtualną konsolę z dostępem do myszy, klawiatury, • Wsparcie dla IPv6, • Wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish, • Możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, • Możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer, • Integracja z Active Directory, • Możliwość obsługi przez dwóch administratorów jednocześnie, • Wsparcie dla dynamic DNS, • Wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, • Możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera, • Możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera.
Certyfikaty	<p>Serwer musi posiadać deklaracja CE.</p>
Warunki gwarancji	<p>7 lat gwarancji producenta, z czasem reakcji 4 godziny od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p>
Dokumentacja użytkownika	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p>



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

B. Serwer typ 2 – ilość: 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max. 1U wyposażona w komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów 3rd Generacji Intel Xeon.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane dwa procesory z serii GOLD min. 8-rdzeniowe klasy x86, min. 3.2GHz
RAM	Minimum 512GB DDR4 RDIMM 3200MT/s w modułach min. 32GB, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC
Gniazda PCI	Min. 2 sloty PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe). Dodatkowo zainstalowane: <ul style="list-style-type: none"> • 2 interfejsy 10/25GB w standardzie SFP28, • 2 interfejsy FC 16 Gbps.
Dyski twarde	Zainstalowane 2 dyski M.2 SATA o pojemności min. 240GB Hot-Plug w konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.
Wbudowane porty	Min. 3 porty USB, w tym min. 1 port USB 3.0 Min. 2 porty VGA, Możliwość rozbudowy o Serial Port
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 800W każdy.
System operacyjny/dodatkowe oprogramowanie	Microsoft Windows Server 2022 Datacenter z dostępowością dla 50 użytkowników (lub równoważny), Microsoft SQL Server 2019 Standard (4-core) lub równoważny.



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

Bezpieczeństwo	<ul style="list-style-type: none"> • Blokada służąca do ochrony nieautoryzowanego dostępu do dysków twardych, • Możliwość wyłączenia w BIOS funkcji przycisku zasilania, • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła, • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą, • Moduł TPM 2.0, • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera, • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.
Diagnostyka	Serwer wyposażony w panel LCD umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:</p> <ul style="list-style-type: none"> • Zdalny dostęp do graficznego interfejsu Web karty zarządzającej, • Zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera), • Szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika, • Możliwość podmontowania zdalnych wirtualnych napędów, • Wirtualną konsolę z dostępem do myszy, klawiatury, • Wsparcie dla IPv6, • Wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish, • Możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, • Możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer, • Integracja z Active Directory, • Możliwość obsługi przez min. dwóch administratorów jednocześnie, • Wsparcie dla dynamic DNS, • Wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, • Możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera, • Możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera.
Certyfikaty	Serwer musi posiadać deklarację CE.
Warunki gwarancji	<p>7 lat gwarancji producenta, z czasem reakcji 4 godziny od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365</p> <p>W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p>
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

C. Środowisko wirtualne (dotyczy pozycji A i B) wraz z instalacją i konfiguracją:

System powinien umożliwiać uruchamianie wirtualizacji (pełne wykorzystanie procesorów i pamięci operacyjnej) na trzech maksymalnie dwuprocessorowych serwerach fizycznych, oraz jednej konsoli do zarządzania całym środowiskiem.

System powinien być dostarczony wraz z wsparciem na 36 miesięcy, świadczonym przez producenta wirtualizacji:

- i. Warstwa wirtualizacji powinna być rozwiązaniem systemowym tzn. powinna być zainstalowana bezpośrednio na sprzęcie fizycznym,
- ii. Rozwiązanie powinno zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej,
- iii. Wirtualizacja musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do min 6TB pamięci operacyjnej,
- iv. Wirtualizacja musi zapewnić możliwość skonfigurowania maszyn wirtualnych do 128 procesorów wirtualnych każda z krokiem co jeden,
- v. Rozwiązanie powinno umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług,
- vi. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej,
- vii. Rozwiązanie powinno wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 7, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008R2, Windows Server 2012, Windows Server 2016, RHEL w wersjach 3.x do 7.x, Debian w wersjach 6x – 9.x, CentOS w wersjach 5.x – 7.x, Oracle Linux w wersjach 4.9 – 7.x, FreeBSD w wersjach 7.x – 11.x, Ubuntu, SCO OpenServer, SCO Unixware (każdorazowo dopuszczalne są rozwiązania równoważne),
- viii. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i usługami,
- ix. Rozwiązanie powinno zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej,
- x. Wirtualizacja powinna zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy,
- xi. Wirtualizacja powinna zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi,
- xii. System zarządzający musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi Microsoft Active Directory (lub równoważnymi),
- xiii. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych aniżeli fizycznie zarezerwowane,
- xiv. Rozwiązanie powinno umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury,
- xv. Rozwiązanie powinno zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej tak, aby zminimalizować ryzyko awarii systemu na skutek wprowadzenia zamiany.

D. Wysoka dostępność:

- i. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych.
- ii. Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury.
- iii. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.
- iv. Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jaki zmianę jej wersji.



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

8. Macierz wraz z konfiguracją – ilość: 1 sztuka

1	Wymagania techniczne
1.1	<p>Obudowa - gęstość upakowania:</p> <ul style="list-style-type: none"> Możliwość zainstalowania w standardowej szafie RACK min. 19", Urządzenie musi wykorzystywać półki dyskowe wysokiej gęstości upakowania - co najmniej 24 dyski na 2U wysokości dla dysków 2,5 cala oraz półki dyskowe zawierające co najmniej 12 dysków 3,5 cala na wysokości 2U, Urządzenie musi wykorzystywać półki dyskowe wysokiej gęstości umożliwiające upakowanie co najmniej 90 dysków na maksymalnej wysokości 5U.
1.2	<p>Zarządzanie:</p> <ul style="list-style-type: none"> Urządzenie musi umożliwiać zarządzanie za pomocą interfejsu Ethernet, Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej, Funkcjonalność bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje, Interfejs zarządzający GUI, CLI oraz zapewnienie możliwości tworzenia skryptów użytkownika.
1.3	<p>Ilość portów:</p> <ul style="list-style-type: none"> Wymagane jest nie mniej niż 4 porty 1Gb Ethernet Base-T oraz 8 portów 16Gb FC wyposażonych we wkładki SFP+ 16Gb SWL.
1.4	<p>Obsługa dysków:</p> <ul style="list-style-type: none"> Musi obsługiwać dyski SAS: <ul style="list-style-type: none"> o prędkościach obrotowych 10000 obr./min. i pojemnościach 1.2TB, 1.8TB, 2.4TB, o prędkościach obrotowych 7200 obr./min. i pojemnościach 2TB, 4TB, 6TB, 8TB, 10TB, 12TB, 14TB, 16TB, Musi obsługiwać dyski SSD o pojemnościach 800 GB, 1.92 TB, 3.84 TB, 7.68 TB, 15.36 TB, 30.72 TB, Musi obsługiwać, co najmniej 380 dysków na parę kontrolerów z zastosowaniem dodatkowych półek. Macierz musi umożliwiać rozbudowę o pojedyncze dyski fizyczne i pojedyncze półki rozszerzeń, Musi umożliwiać konfigurację, która w jednym rozwiązaniu łączyć będzie półki rozszerzeń na dyski 2,5" z półkami na dyski 3,5".
1.5	<p>Pojemność dyskowa:</p> <p>Macierz dyskowa musi być wyposażona w minimum: 7 dysków o pojemności 3,84TB SSD.</p>
1.6	<ul style="list-style-type: none"> Macierz musi zapewnić możliwość wymiany uszkodzonych dysków podczas pracy systemu (Hot-Swap). Macierz musi umożliwiać stworzenie konfiguracji odpornej na awarię pojedynczego dysku oraz odporność na awarię dwóch dysków. Przestrzeń zapasowa powinna być realizowana za pomocą przestrzeni zapasowej rozmieszczonej na wszystkich dyskach w ramach grupy RAID lub w formie dysku nadmiarowego.
1.7	<p>Obsługa pamięci Cache:</p> <p>Macierz musi być wyposażona w minimum 32GB pamięci Cache, z możliwością rozbudowy do 64GB, Pamięć cache w 95% musi być przeznaczona na obsługę operacji wejścia/wyjścia.</p>
1.8	<p>Wsparcie dla systemów operacyjnych:</p> <p>Macierz musi wspierać następujące systemy operacyjne i wirtualizatory: MS Windows Server Vmware vSphere, RedHat Enterprise Linux, Suse (każdorazowo dopuszczalne są rozwiązania równoważne)</p>



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

2	Dodatkowe wymagania i funkcjonalności:
2.1	<p>Funkcje niezawodnościowe:</p> <ul style="list-style-type: none"> • Wszystkie krytyczne komponenty urządzenia takie jak: kontrolery dyskowe, pamięć cache, zasilacze i wentylatory muszą być zdublowane tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu, • Komponenty te muszą być wymienne w trakcie pracy macierzy, • Urządzenie musi cechować brak pojedynczego punktu awarii, • Wsparcie dla zasilania z dwóch niezależnych źródeł prądu poprzez nadmiarowe zasilacze typu Hot-Swap, • Wentylatory typu Hot-Swap, • Wbudowane co najmniej dwa kontrolery RAID, • Urządzenie musi posiadać pamięć typu Flash dla zapisu danych z pamięci cache na wypadek zaniku zasilania oraz system podtrzymania zasilania pozwalający na zapis danych z cache do pamięci typu Flash.
2.2	<p>Funkcjonalności:</p> <ul style="list-style-type: none"> • Musi istnieć funkcjonalność Cache dla procesu odczytu, • Musi istnieć funkcjonalność Mirrored Cache dla procesu zapisu, • Możliwość wyłączenia cache dla poszczególnych wolumenów, • Funkcjonalność partycjonowania pamięci cache, • Funkcjonalność separacji przestrzeni dyskowych pomiędzy różnymi podłączonymi hostami, • Funkcjonalność dynamicznego zwiększania i zmniejszania rozmiaru wolumenów, • Funkcjonalność zarządzania ilością operacji wejścia/wyjścia wykonywanych na danym wolumenie – zarządzanie musi być możliwe zarówno poprzez określenie ilości operacji I/O na sekundę jak również przepustowości określonej w MB/s, • Urządzenie musi obsługiwać funkcjonalność ochrony przed skasowaniem lub odmapowaniem od hosta woluminu dyskowego, do którego były przesłane operacje wejścia/wyjścia w określonym przez użytkownika czasie, • Dostępne sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu dla podłączanych systemów operacyjnych.
2.3	<p>Obsługa wirtualnych dysków logicznych:</p> <ul style="list-style-type: none"> • Minimalna ilość wspieranych wirtualnych dysków logicznych (LUN) dla całej (globalnej) puli dyskowej musi wynosić co najmniej 2000. Funkcjonalność LUN Masking i LUN Mapping.
2.4	<p>Funkcjonalność thin provisioning:</p> <ul style="list-style-type: none"> • Urządzenie musi obsługiwać funkcjonalność thin provisioning dla wszystkich wolumenów. • Musi istnieć możliwość wyłączenia tej funkcjonalności dla wybranych wolumenów. • Należy dostarczyć rozwiązanie umożliwiające korzystanie z funkcji thin provisioning na całą oferowaną pojemność urządzenia.
2.5	<p>Kopie migawkowe:</p> <ul style="list-style-type: none"> • Urządzenie musi mieć możliwość wykonywania natychmiastowej kopii danych (point-in-time copy). • Funkcjonalność ta powinna być realizowana w trybie copy-on-write. • Rozwiązanie powinno obejmować możliwość stworzenia co najmniej 60 kopii.
2.6	<p>Migracja wolumenów logicznych:</p> <ul style="list-style-type: none"> • Urządzenie musi mieć możliwość wykonania migracji wolumenów logicznych pomiędzy różnymi typami dysków wewnątrz macierzy bez zatrzymywania aplikacji korzystającej z tych wolumenów. • Wymaga się, aby zasoby źródłowe podlegające migracji oraz zasoby, do których są migrowane mogły być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (SAS, SSD, SATA).



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

2.7	<p>Replikacja macierzy:</p> <ul style="list-style-type: none"> • Urządzenie musi posiadać funkcjonalność replikacji danych przy użyciu synchronicznych oraz asynchronicznych transmisji danych przez łącza komunikacyjne IP oraz FC. • Oba rodzaje replikacji muszą wspierać program Vmware Site Recovery Manager do odzyskiwania danych po awarii.
2.8	<p>Wirtualizacja zasobów:</p> <ul style="list-style-type: none"> • Macierz musi mieć możliwość wirtualizacji zasobów znajdujących się na innych niż oferowane macierze dyskowe na potrzeby migracji danych. • Migracja musi się odbyć w trybie bezprzerwowym.
2.9	Macierz musi mieć funkcjonalność wykonywania pełnej kopii lokalnych wolumenów logicznych z wykorzystaniem jedynie kontrolerów macierzy. Rozwiązanie powinno obejmować możliwość stworzenia co najmniej 60 kopii.
2.10	Macierz musi mieć możliwość dodawania kolejnych półek dyskowych oraz dysków bez przerywania pracy macierzy, dla dowolnej konfiguracji macierzy
2.11	<ul style="list-style-type: none"> • Macierz musi posiadać funkcjonalność optymalizacji wykorzystania dysków SSD/Flash poprzez automatyczną identyfikację najbardziej obciążonych fragmentów wolumenów w zarządzanych zasobach dyskowych oraz ich automatyczną migrację na dyski SSD/Flash. • Macierz musi również automatycznie rozpoznawać obciążenie fragmentów wolumenów na dyskach SSD/Flash i automatycznie migrować z dysków SSD/Flash nieobciążone fragmenty wolumenów. • Macierz musi posiadać możliwość wykorzystania mechanizmu optymalizacji umiejscowienia danych pomiędzy przynajmniej 3 rodzajami dysków – SSD/Flash, Enterprise (SAS 10k) oraz NL-SAS/SATA, jak również przy wykorzystaniu dwóch dowolnych z wyżej wymienionych typów. • Opisany powyżej proces optymalizacji musi posiadać funkcję włączenia/wyłączenia na poziomie pojedynczego wolumenu.
2.12	Macierz musi mieć możliwość aktualizacji oprogramowania macierzy (firmware) w trybie online.
2.13	Macierz musi umożliwiać tworzenie wolumenów o pojemności nie mniejszej niż 250 TB
2.14	Do macierzy należy dołączyć przewody zasilające oraz 8 przewodów światłowodowych o długości 5m.
3	Inne:
3.1	Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu.
3.2	Oferowane produkty (urządzenia, sprzęty) muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE.
3.3	Urządzenie musi współpracować z siecią energetyczną o parametrach w przedziale 200V- 230V, 50 Hz.
3.4	Urządzenie musi być objęte serwisem gwarancyjnym przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania (w tym wbudowanego) oraz wsparcie techniczne w trybie 24x7.
3.5	Zgłoszenia usterek muszą być akceptowane przez producenta zarówno drogą email jak również drogą telefoniczną. Linia telefoniczna musi być czynna 24 godziny na dobę, 7 dni w tygodniu również w dni świąteczne.

9. Okablowania strukturalne wraz z osprzętem i z instalacją:

- Gwarancja na wykonane prace i zastosowane materiały sieci LAN – 3 lata,
- Kabel STP kat. 6A - 15 960 mb,
- Kabel UTP kat. 5E - 500 mb,
- Kabel światłowodowy 12 włókien MM 50/125 OM3 - 900 mb,
- Niezbędne materiały montażowe,



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

- Szafa serwerowa RACK 19 cali 42U 800x1000 mm – 2 szt.
- Szafa serwerowa RACK 19 cali 27U 800x800 mm – 1 szt.
- Szafa serwerowa RACK 19 cali 27U 800x800 mm IP 55 – 1 szt.
- Wyposażenie szaf:
 - Listwy zasilające - 5 szt.
 - Panele wentylacyjne - 8 szt.
 - Panele światłowodowe - 4 szt.
 - Panele krosowe z modułami keystone RJ45 - 18 szt.
 - Panele wieszakowe - 20 szt.
 - Kable krosowe - 576 szt.

10. Systemy do wizualizacji informacji wraz z konfiguracją – ilość: 4 sztuki

- Gwarancja i wsparcie serwisowe 2 lata,
- Wielkość ekranu co najmniej 85”,
- Rozdzielczość 4K,
- Zewnętrzny komputer z procesorem i5 z serii co najmniej 8 - 8 GB RAM, 250 SSD, Windows 11.

11. Punkty dostępowe dla operatorów i inżynierów produkcji – komputery – ilość: 20 sztuk

- Urządzenie typu All in One,
- Gwarancja i wsparcie serwisowe 5 lat,
- Gwarancja Keep Your Hard Drive lub równoważna,
- Usługa ochrony przed przypadkowymi uszkodzeniami,
- Ekran dotykowy wielkości co najmniej 21” z folią zabezpieczającą,
- Procesor i5 z serii co najmniej 8 generacji,
- Co najmniej 16GB RAM,
- Co najmniej dysk 256 GB SSD,
- Ethernet 1GB,
- Możliwość instalacji systemu operacyjnego Windows 11,
- Możliwość zawieszenia na wieszaku VESA + uchwyt,
- Czytnik kodów kreskowych i QR,
- Czytnik RFID.

12. Punkty dostępowe dla operatorów i inżynierów produkcji – tablety – ilość: 2 sztuki

- Gwarancja i wsparcie serwisowe 2 lata,
- Obudowa typu Rugged,
- Obudowa z klasą szczelności co najmniej IP65,
- Procesor i5 z serii co najmniej 8 generacji,
- Wielkość ekranu 10” -11”,
- Co najmniej 8GB RAM,
- System operacyjny Windows 10/11 (lub równoważny),
- Dysk co najmniej 128 GB SSD,
- Czytnik kodów kreskowych i QR,
- Czytnik RFID,
- Możliwość zawieszenia na wieszaku VESA + uchwyt.



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice

Konfiguracja/Instalacja/Montaż**Infrastruktura sieciowa:**

- Konfiguracja infrastruktury opartej o kontroler, punkty dostępowe oraz przełączniki,
- Konfiguracja vlanów (router + switche dostępowe),
- Konfiguracja polityk dostępowych (pomiędzy vlanami, do internetu),
- Migracja urządzeń końcowych do vlan,
- Wdrożenie funkcji bezpieczeństwa (antywirus, IPS, Web/DNS filtering),
- Wdrożenie rozwiązania do dwuetapowego logowania,
- Przygotowanie dokumentacji powykonawczej.

Serwery:

- Montaż serwerów w szafie rack i instalacja okablowania zgodnie z wytycznymi Zamawiającego,
- Upgrade oprogramowania serwerów (firmware), konfiguracja kart zarządzających zdalnego zarządzania (zarządzanie sprzętowe),
- Konfiguracja RAID1 dla wolumenów (dyski M.2) dla potrzeb instalacji wirtualizacji,
- Zamontowanie i konfiguracja wolumenów wystawionych z macierzy dla potrzeb klastra wirtualizacji,
- Konfiguracja klastra i elementów HA (wysokiej dostępności) tak, by w sytuacji awarii serwera nastąpiło automatyczne uruchomienie maszyn wirtualnych na sprawnym serwerze klastra.
- Konfiguracja mechanizmów migracji wirtualnych maszyn w ramach klastra bez konieczności wyłączania ich.

Macierz:

- Montaż macierzy w szafie rack i instalacja okablowania zgodnie z wytycznymi Zamawiającego,
- Uruchomienie i inicjalizacja macierzy: uzupełnienie danych o macierzy (nazwa etc.), Ustawienie adresów IP, stworzenie cluster node, utworzenie pul dyskowych oraz wolumenów w technologii RAID,
- Prezentacja zasobów do hostów Wirtualizacji: konfiguracja połączeń pomiędzy hostami a macierzą w sposób zapewniający redundancję, udostępnienie współdzielonych zasobów do obu hostów za pomocą połączeń FC,
- Szkolenie z obsługi i konfiguracji ustawień macierzy,
- Przeprowadzenie szkolenia z obsługi, interfejsu i konfiguracji ustawień macierzy,
- Sporządzenie i przekazanie dokumentacji powdrożeniowej w wersji elektronicznej.

Uwagi

Wszystkie sformułowania zawarte powyżej, odnoszące się do czynności związanych z konfiguracją lub instalacją lub montażem, które będą wykonywane przez Wykonawcę, należy rozumieć jako pomocnicze usługi obce, które są niezbędne do realizacji dostawy przedmiotu zapytania ofertowego, a tym samym nieposiadające znamion zewnętrznej usługi merytorycznej.



Fabryka Armatur „Swarzędz” sp. z o.o.
ul. Świerkowa 27
62-020 Rabowice