Nr postępowania:
ZP.271.9.2022

Załącznik nr 8 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

(OPZ)

dla postępowania o udzielenie zamówienia klasycznego
w trybie podstawowym
przewidzianym w art. 275 pkt 1
ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych

Dostawa sprzętu komputerowego w ramach projektu Cyfrowa Gmina

Zadanie jest dofinansowane w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020
Oś Priorytetowa V: Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU
działanie 5.1: Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia
z projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00-0001/21-00

1. Przedmiotem zamówienia jest dostawa:
   - 16 szt. komputerów przenośnych,
   - 1 szt. zapory serwerowej typu UTM,
   - 1 szt. serwera pamięci dyskowej, w ramach doposażenia serwerowni i jej rozbudowy

   w ramach projektu Cyfrowa Gmina.
   W Specyfikacji produktów (załącznik nr 1A do SWZ) należy podać model, typ i nazwę producenta oferowanego sprzętu.

2. Minimalne wymagane parametry techniczne dla komputerów przenośnych

Lp.	Nazwa komponentu	Minimalne wymagane parametry techniczne
1	Typ	Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości FHD (1920x1080) IPS w technologii LED przeciwodblaskowy,
2	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
3	Procesor	Procesor klasy x86, 2 rdzeniowy, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem, co najmniej 3,00 GHz, z pamięcią cache L3 co najmniej 6 MB, TDP: 12W (down) i 28W (up) lub równoważny 2 rdzeniowy procesor klasy x86
4	Pamięć operacyjna RAM	1 x 8GB DDR4-2666, min. jeden slot wolny na dalszą rozbudowę, możliwość rozbudowy do min 16GB
5	Parametry pamięci masowej	256 GB SSD M.2 NVMe
6	Karta graficzna	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej, ze sprzętowym wsparciem dla DirectX 12
7	Wyposażenie multimedialne	Karta dźwiękowa stereo, wbudowane 2 głośniki (stereo) Wbudowany w obudowę matrycy mikrofon wraz z kamerą
8	Wymagania dotyczące baterii i zasilania	40WHr, Li-Ion. wspierająca funkcję szybkiego ładowania. Czas pracy na baterii wg dokumentacji producenta min 6 godzin Zasilacz o mocy min. 45W
9	Zgodność z systemami operacyjnymi i standardami	Zgodność z 64-bitową wersją systemu operacyjnego Microsoft Windows 10 Home PL, zainstalowany system operacyjny niewymagający aktywacji za pomocą telefonu lub Internetu w firmie Microsoft
10	Certyfikaty i standardy	Certyfikat ISO9001:2000 dla producenta sprzętu Certyfikat ISO 14001 dla producenta sprzętu
11	Waga, wymiary i obudowa	Waga max 2.1 kg z baterią Dioda sygnalizująca pracę dysku. Dioda sygnalizująca stan zasilania.
12	BIOS	BIOS zgodny z UEFI. Możliwość odczytania z BIOS: – Wersji BIOS – Modelu procesora, prędkości procesora, – Informacji o ilości pamięci RAM – Informacji o fabrycznie zainstalowanym systemie operacyjnym – Informacji o: numerze seryjnym, ID płyty głównej.

		– Informacji o preinstalowanym systemie operacyjnym. – Informacji o baterii: numer seryjny oraz data produkcji. Możliwość wyłączenia/włączenia: wirtualizacji, z poziomu BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Ustawienia hasła Administratora oraz Power-On bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Możliwość ustawienia hasła na dysk Możliwość włączenia/wyłączenia TPM Możliwość włączenia/wyłączenia: – Karty sieciowej LAN – Karty sieci bezprzewodowej WiFi – Bluetooth – Czytnika kart SD – Mikrofonu Możliwość ustawienia pracy portów USB podczas POST w tryb: – Zezwól na działanie wszystkich portów – Zezwól na działanie tylko klawiatury i myszki podłączonej do portów USB – Zezwól na wszystkie urządzenia oprócz pamięci masowych i hubów USB
13	Warunki gwarancji	2 letnia gwarancja producenta onsite Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta
14	Wymagania dodatkowe	Wbudowane porty i złącza: 1 x HDMI 1.4b, 3 szt USB Karta sieciowa LAN 10/100/1000 Ethernet RJ 45 zintegrowana z płytą główną oraz WLAN 802.11b/g/n/AC + Bluetooth 4.2 (COMBO). Klawiatura (układ US -QWERTY), min 102 klawisze z wydzieloną strefą klawiszy numerycznych. Touchpad

3. Minimalne wymagane parametry techniczne dla zapory serwerowej typu UTM

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa 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.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu,

Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 16 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 1518 B.
3. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 64 B.
4. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
6. Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.
7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.

3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Analiza ruchu szyfrowanego protokołem SSH.
13. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityka, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - Nuage Networks VSP.
   - OpenStack.
   - VMware vCenter (ESXi).
   - VMware NSX.
   - VMware NSX.Nutanix
   - VMware NSX.IBM Cloud

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).

- Obsługa protokołu Diffie-Hellman grup 19 i 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - 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.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie powinno zapewniać obsługę:

- Routingu statycznego.
- Policy Based Routingu.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
3. Rozwiązanie powinno wspierać funkcję Forward Error Correctionm na tunelach IPSec.
4. Funkcja monitorowania łącza w oparciu o rzeczywisty ruch bez konieczności tworzenia dedykowanych detektorów.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu

Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

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

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.

7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
9. Filtrowanie treści wideo w oparciu o kategorie - co najmniej dla servisów youtube, vimeo.
10. Blokowanie wysyłania poświadczeń firmowych do obcych serwisów.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

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

- Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Gwarancja oraz wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 24 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. Minimalne wymagane parametry techniczne serwera pamięci dyskowej (doposażenie serwerowni i jej rozbudowa)

Lp.	Nazwa komponentu	Minimalne wymagane parametry techniczne
1	Obudowa	Możliwość zainstalowania w standardowej szafie rack 19" nie będącej przedmiotem zamówienia. Rozmiar jednostek sterującej nie może przekraczać 2U . Dodawanie kolejnych półek lub dysków musi odbywać się bezprzerwowo. Całkowity rozmiar dostarczonej macierzy nie może przekraczać 2U.
2	Kontrolery	Wymagane dwa moduły sterujące pracujące w trybie active-active. W przypadku wystąpienia awarii sprawny moduł musi automatycznie przejąć obsługę wszystkich zasobów prezentowanych przez serwer dyskowy.
3	Dostępne porty	Oferowany serwer dyskowy musi posiadać w chwili dostawy minimum 4 porty SAS 12Gbs powalających na podłączenie dwóch serwerów w sposób redundantny, oraz minimum 4 porty 10GB iSCSI . Te same porty powinny umożliwiać podłączenie do sieci FC z prędkością 16Gbs. Jeżeli oferowany serwer dyskowy nie dopuszcza takiej możliwości to Zamawiający zezwala na dostarczenie serwera dyskowego, który posiada 4 porty 16Gb FC oraz minimum 4 porty 10Gb iSCSI .
4	Cache	Każdy z modułów sterujących musi być wyposażony w min 8 GB pamięci cache zabezpieczonej mechanizmem mirroringu. Pamięć podręczna musi być zabezpieczona przed utratą danych w przypadku zaniku zasilania. Rozwiązania wykorzystujące do tego celu tylko i wyłącznie tzw. podtrzymanie cache za pomocą baterii nie są akceptowalne. Bateria może być użyta tylko i wyłącznie na czas zrzutu danych z cache na pamięć nieulotną. Ponadto serwer dyskowy musi umożliwiać utworzenie dedykowanej przestrzeni SSD stanowiącej pamięć cache pośredniczącą w operacjach odczytów danych. Wymaga się

		możliwości utworzenia takiej przestrzeni o wielkości 4TB.
5	Dyski	Serwer dyskowy musi obsługiwać dyski twarde typu SSD oraz dyski obrotowe SAS, NL-SAS. Serwer dyskowy musi być wyposażony w minimum 4 dyski SAS 10K o pojemności minimum 1,2TB Serwer dyskowy musi umożliwiać instalację do minimum 96 dysków 2,5”
6	Funkcjonalność	Serwer dyskowy musi obsługiwać typy protekcji RAID 0, 1, 3, 5, 6, 10 oraz powinien posiadać funkcjonalność zarządzania informacjami o parzystości oraz dyskami spare w całej puli dysków utworzonej ze wszystkich dysków, które mogą zostać zainstalowane w serwerze dyskowym. W przypadku awarii dysku, do jego obudowy musi być używany każdy dysk z takiej puli Serwer dyskowy musi umożliwiać zwiększanie i zmniejszanie online pojemności poszczególnych wolumenów logicznych oraz dynamiczne alokowanie przestrzeni dyskowej (tzw. „*thin provisioning*”). Serwer dyskowy musi mieć możliwość replikacji danych po FC w trybie asynchronicznym. Serwer dyskowy musi pozwalać na wykonanie do 32 jednoczesnych replikacji bez używania systemów zewnętrznych wykonujących replikację. Nie wymaga się funkcjonalności replikacji w momencie dostawy. Wymagana możliwość definiowania globalnych dysków hot-spare. Wymagana możliwość logicznej zamiany dysków z wykorzystaniem dysków nieprzypisanych. Serwer dyskowy musi posiadać automatyczny monitoring z możliwością informowania o awariach poprzez protokół smtp oraz snmp oraz możliwość wysyłania powiadomień awarii do wskazanych odbiorców. Wysyłane powiadomienia muszą zawierać nazwę serwera dyskowego, informację o typie zdarzenia, datę i czas wystąpienia zdarzenia oraz krótki opis zdarzenia. Serwer dyskowy musi mieć możliwość definiowania poziomu zajętości miejsca, po osiągnięciu którego nastąpi wysłanie powiadomienia pod wskazane adresy email. System zarządzania powinien posiadać funkcjonalność kreatora konfiguracji uruchamianego automatycznie w przypadku braku zdefiniowanych pul dyskowych i wolumenów, w przypadku braku zdefiniowanych powiadomień. Serwer dyskowy musi mieć funkcjonalność automatycznej detekcji podłączonych hostów (nazwa hosta oraz typ systemu operacyjnego). Musi być możliwość edycji hostów dodanych w sposób automatyczny. Wymagana jest funkcjonalność automatycznego tworzenia przestrzeni dyskowych zoptymalizowanych pod katem używanych na nich aplikacji jak SQL Server, Exchange oraz Vmware vmfs. Serwer dyskowy musi mieć możliwość definiowania priorytetu operacji wprowadzanych zmian konfiguracji w odniesieniu do obciążenia generowanego przez podłączone hosty. Wymagana jest możliwość sprawdzenia aktualnych zadań serwera dyskowego. Serwer dyskowy musi umożliwiać szyfrowanie zapisywanych na nim danych poprzez dodanie dysków samoszyfrujących. Nie wymaga się tej funkcjonalności w chwili dostawy. Serwer dyskowy musi posiadać możliwość fizycznej identyfikacji (dioda LED) aktywowanej z interfejsu zarządzania oraz funkcjonalność fizycznego identyfikowania dysków (dioda LED) należących do jednej przestrzeni logicznej. Serwer dyskowy musi mieć możliwość przypisania wolumenu danych tylko do wybranego hosta należącego do zdefiniowanego klastra.
7	Wydajność	Wymaga się możliwości rozbudowania serwera dyskowego do poziomu wydajności przynajmniej 99 000 operacji wejścia wyjścia dla losowego odczytu oraz przynajmniej 34 000 operacji wejścia wyjścia dla losowego zapisu. Wymagana pojemność dla wolumenów z dynamiczną alokacją przestrzeni to przynajmniej 256 TB
8	Zarządzanie serwerem dyskowym	Dostępne dwa porty 1Gbe Base-T w trybie primary/redundant. Zarządzanie serwerem dyskowym powinno być możliwe za pomocą graficznego interfejsu użytkownika dostępnego poprzez protokół https, oraz za pomocą linii komend cli osiągalnej poprzez protokół ssh.

		Interfejs zarządzania powinien wylogować sesje po maksymalnie 15 minutach bezczynności. Maksymalna ilość prób podania hasła administratora nie może być większa niż 5 do momentu zablokowania dostępu. Wymagana możliwość autentykacji poprzez LDAP oraz funkcjonalność role-based access control. Wymaga się możliwości definiowania przynajmniej następujących poziomów dostępu: - storage admin – pełen dostęp wyłączeniem ustawień bezpieczeństwa - security admin – dostęp do ustawień bezpieczeństwa - support admin – pełen dostęp serwisowy - monitor – możliwość odczytu konfiguracji
9	Inne	Wymagana jest bezprzerwowa wymiana następujących elementów serwera dyskowego: kontrolery, moduły I/O, dyski, zasilacze oraz moduły SFP+. Wymaga się możliwości integracji serwera dyskowego z systemem zarządzania infrastrukturą, opisanym w sekcji Serwery Do serwera należy dostarczyć 4 kable producenta MiniSAS HD 8644/MiniSAS HD 8644 o długości 0,5m. Obsługa systemów operacyjnych hosta: Microsoft Windows Server 2012 R2, 2016, 2019; Red Hat Enterprise Linux (RHEL) 6, 7, 8; SUSE Linux Enterprise Server (SLES) 11, 12, 15; VMware vSphere , 6.5, 6.7, 7.0
10	Gwarancja	Co najmniej 2 letnie wsparcie w trybie on-site. Gwarancja producenta, serwis w miejscu instalacji sprzętu świadczony przez producenta serwera lub autoryzowanego partnera serwisowego. Możliwość wykupienia dodatkowego wsparcia zapewniającego okno zgłoszeń 24x7 oraz gwarantowany czas naprawy sprzętu do 24 godzin.

Na potwierdzenie zgodności oferowanych dostaw z wymaganiami, cechami lub kryteriami określonymi w Opisie Przedmiotu Zamówienia, Zamawiający żąda złożenia Przedmiotowych Środków Dowodowych w postaci specyfikacji produktu – zgodnie z załącznikiem 1A do SWZ. Specyfikacja Produktu musi zawierać informacje o wszystkich wymienionych w OPZ komponentach komputerów przenośnych, zapory serwerowej typu UTM oraz serwera pamięci dyskowej i potwierdzać spełnienie wszystkich minimalnych wymagań i parametrów tam wskazanych.

Przedmiotowe środki dowodowe, o których mowa w art. 104-107 ustawy pzp, Wykonawca składa wraz z ofertą. Jeżeli Wykonawca nie złoży przedmiotowych środków dowodowych lub będą one niekompletne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie, z zastrzeżeniem art. 107 ust. 3 ustawy pzp.

Wykonawcy mogą zaproponować rozwiązania równoważne o takich samych parametrach lub je przeważające, jednak ich obowiązkiem jest udowodnienie równoważności. W przypadku braku dokumentów udowadniających równoważność, Zamawiający przyjmuje, że oferta nie spełnia wymagań SWZ i zostanie odrzucona.