Załącznik nr 8a do SIWZ

Opis przedmiotu zamówienia – Zadanie nr 1

1. Przedmiot zamówienia obejmuje dostawę zespołu serwerów wraz z systemem zabezpieczeń
2. Szczegółowa specyfikacja techniczna przedmiotu dostaw:

1) SERWER – 1 sztuka

L.p.	Element konfiguracji	Wymagania minimalne
1	Obudowa	Maksymalnie 1U RACK 19 cali (wraz z szynami umożliwiającymi wysunięcie i wszystkimi elementami niezbędnymi do zamontowania serwera w szafie oraz ramieniem do prowadzenia kabli)
2	Procesor	Minimum szesnastordzeniowy, o częstotliwości min. 2,1 GHz osiągający w testach SPECint_rate2006 w kolumnie Result wynik nie gorszy niż 1340 punktów dla serwera w konfiguracji dwuprocesorowej. Wynik testu musi być publikowany na stronie www.spec.org
3	Liczba procesorów	Minimum 2
4	Pamięć operacyjna	Minimum 256 GB RDIMM DDR4, z możliwością rozbudowy do minimum 3TB. Minimum 24 sloty na pamięć. Zabezpieczenia pamięci: Advanced ECC oraz Online Spare.
5	Sloty rozszerzeń	Minimum 2 sloty PCI-Express Generacji 3 w tym minimum jeden slot x16 (prędkość slotu – bus width) pełnej wysokości oraz minimum jeden slot x8 (prędkość slotu – bus width). Możliwość rozbudowy o dodatkowy, trzeci slot PCI-Express Generacji 3 x16 (prędkość slotu – bus width).
6	Dysk twardy	Możliwość zainstalowania do 8 dysków typu Hot Swap, SAS/SATA/SSD, 2,5”. Zainstalowane: 2x 300GB 10k rpm SAS. Możliwość rozbudowy/rekonfiguracji serwera do obsługi 10 wewnętrznych dysków 2,5’’.
7	Kontroler	Kontroler macierzowy SAS 12Gb z min. 2GB cache, z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę do 10 napędów dyskowych SAS, obsługujący poziomy: RAID 0/1/1+0/5/5+0/6/6+0. Możliwość rozbudowy pamięci cache do 4GB poprzez

		rozbudowę kontrolera lub wymianę kontrolera.
8	Interfejsy sieciowe	Minimum 4 wbudowane porty Ethernet 1GbE z funkcją Wake-On-LAN, RJ45, niezajmujące slotów PCI-E. Minimum 2 portowa karta sieciowa 10Gb iSCSI nie zajmująca slotu PCI-Express. Wraz z kartą należy dostarczyć komplet wkładek SFP+ SR 10Gb (Multimode). Wkładki muszą być tego samego producenta co oferowany serwer.
9	Karta graficzna	Zintegrowana karta graficzna
10	Porty	5 x USB 3.0 (w tym dwa wewnętrzne). 1x VGA Wewnetrzny slot na kartę microSD/SD. Możliwość rozbudowy o: - dodatkowy porty VGA dostępny z przodu serwera, - port szeregowy,
11	Dodatkowe napędy	Brak
12	Zasilacz	Minimum 2 szt., min. 500W, typ Hot-plug, redundantne o sprawności minimum 94%
13	Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
14	Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty. Karta zdalnego zarządzania musi posiadać wbudowaną pamięć flash, minimum 4GB, w tym minimum 1GB dostępny dla użytkownika serwera. Możliwość rozszerzenia licencji o dodatkowe funkcjonalności: przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS), przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD/DVD/ISO i FDD. Licencja na obecnym etapie nie jest wymagana. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną, posiadające dedykowany port RJ45.
15	Wsparcie dla Systemów Operacyjnych i Systemów Wirtualizacyjnych	Microsoft Windows Server Canonical Ubuntu Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware Citrix XenServer Oracle Linux
16	Gwarancja i wsparcie	3 lata w miejscu instalacji, z czasem reakcji maksymalnie w następnym dniu roboczym od zgłoszenia (NBD), tryb zgłaszania 9x5.
17	Inne	• Wraz z serwerem należy dostarczyć dwie, 2-

		portowe karty HBA z portami zewnętrznymi 12Gb/s. Karty muszą być kompatybilne z zamawianym serwerem • Wraz z serwerem należy dostarczyć dodatkowo jedną dwuportową kartę sieciową o parametrach: -10GbE - 2x SFP+ - kontroler typu Intel 82599 lub zgodny - interfejs PCI-E - komplet (2 szt.) kompatybilnych wkładek SFP+ (Multimode)

2) Macierz dyskowa - 1 sztuka

L.p.	Element konfiguracji	Wymagania minimalne
1	Obudowa	System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19".
2	Pojemność:	System musi zostać dostarczony w konfiguracji zawierającej minimum: 2 dyski 800GB SSD, wykonanych w standardzie nie gorszym niż eMLC, z interfejsem 12Gb/s Oraz 14 dysków 900GB SAS z interfejsem 12Gb/s System musi ponadto wspierać dyski: - SAS: 900GB, 1200GB, 1800GB - SATA/NL-SAS: 4TB, 6TB, 8TB, 10TB - SSD: 800GB, 1,6TB, 3,2TB System musi mieć możliwość rozbudowy do minimum 175 dysków oraz musi pozwalać na rozbudowę do wyższych modeli bez potrzeby migracji danych.
3	Kontroler	Dwa kontrolery wyposażone w przynajmniej 8GB cache każdy. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash.
4	Interfejsy	Oferowana macierz musi mieć minimum: 4 porty 10Gb SCSI 4 porty 1GbE (do zarządzania), 4 porty SAS 12 Gb/s (do podłączenia półek dyskowych)

		Jeśli porty w macierzy wymagają instalacji odpowiednich wkładek do realizacji ww. połączeń, zamawiający wymaga ich dostarczenia. System musi pozwalać na rozbudowę o dodatkowe minimum 4 porty 10Gb SCSI. Jeśli dostarczany model macierzy nie ma możliwości rozbudowy o dodatkowe porty 10Gb SCSI zamawiający dopuszcza dostarczenie dwóch przełączników w standardzie 10Gb SCSI, z minimalną obsadą 4 portów 10Gb SCSI (porty muszą posiadać wkładki w momencie dostawy).
5	RAID	Wsparcie dla RAID: 0, 1, 5, 6, 10 Macierz musi posiadać rozwiązanie do szybkiego odtwarzania grup raid po awarii.
6	Obsługiwane protokoły	Macierz musi umożliwiać udostępniaie danych po FC lub iSCSI.
7	Inne wymagania	Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów: Microsoft® Windows Server®, Red Hat Enterprise Linux®, Novell SUSE Linux Enterprise Server, VMware® ESX®, Oracle® Solaris, HP HP-UX, IBM AIX, Macierz musi posiadać funkcjonalność wykonywania snapshotów minimum 128 per wolumen. Macierz musi posiadać funkcjonalność klonowania danych Macierz musi posiadać funkcjonalność replikacji danych po FC w trybie synchronicznym i asynchronicznym, system musi pozwalać na wykonanie do 32 jednoczesnych replikacji Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 128 partycji.

		Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID Macierz musi pozwalać na wykorzystanie dysków SSD w celu akceleracji odczytów. Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków Wraz z system musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście: - wydajności i opóźnień na wolumenach - wydajności I/Ops, MB/s - trafności w cache Macierz musi posiadać oprogramowanie do aplikacji pozwalające na integrację z: - Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter - VMware VASA - VMware Site Recovery Manager – wsparcie dla replikacji macierz z VMware - Microsoft SCOM – integracja systemu macierzowego z monitoringiem i alarmami w Microsoft SCOM - Microsoft MS SQL Management Studio - Microsoft Virtual Disk Service (VDS) - Microsoft Virtual Shadow Service (VSS) - Oracle Enterprise Manager – monitoring zasobów macierzowych Macierz musi zapewniać możliwość szyfrowania danych, realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub dostarczone zewnętrzne urządzenie i oprogramowanie do zarządzania kluczami. Wszystkie licencje na funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy.
8	Gwarancja i serwis	Minimum 3 lata gwarancji oraz serwisu, zapewniając dostawę podzespołu zapasowego na następny dzień roboczy wraz z usługą wymiany na miejscu. Dostarczony serwis musi umożliwiać zgłaszanie awarii w trybie 24x7. Dostarczony system musi posiadać również 3 lat

		subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia. Dyski uszkodzone w okresie gwarancji pozostają własnością zamawiającego.

3) Serwer NAS - 1 sztuka

L.p.	Element konfiguracji	Wymagania minimalne
1	Obsługa dysków twardych	Co najmniej 5 x 3.5"/2.5" SATA 6Gb/s HDD/SSD
2	Porty Sieciowe	Minimum 2 x 10 Gigabit SFP+ LAN oraz minimum 2 x Gigabit RJ45 LAN , Wraz z serwerem NAS należy dostarczyć komplet kompatybilnych wkładek SFP+ (Singlemode)
3	Pamięć	Minimum 4GB DDR3 z możliwością rozbudowy
4	Porty USB	Co najmniej 2 x USB 3.0
5	PCIe Slot	1 x PCIe Gen2 (x2)
6	Masa	Nie więcej niż 6kg (bez dysków)
7	Chłodzenie	Minimum jeden wentylator
8	Zasilanie	ATX 250W, 100-240V AC, 50-60Hz
9	Inne	Z serwerem należy dostarczyć minimum 5 szt. dysków twardych o następujących parametrach: Pojemność minimalna pojedynczego dysku 4 TB SATA 6Gb/s HDD Min. 64 MB cache, Min. 5400 obr/min Dedykowane do pracy w NAS Gwarancja minimum 3 lata na całość (serwer NAS i dyski)

4) Switch 1 sztuka

L.p.	Element konfiguracji	Wymagania minimalne
1	Architektura sieci LAN	10GigabitEthernet
2	Liczba gniazd 10GB SFP+	Minimum 8 szt.
3	Porty komunikacji	Port konsoli
4	Zarządzanie, monitorowanie i konfiguracja	zarządzanie przez przeglądarkę WWW
5	Obsługiwane protokoły	routing statyczny

	routingu	
6	Rozmiar tablicy adresów MAC	Nie mniej niż 16000
7	Prędkość magistrali wew.	Minimum 220 Gb/s
8	Bufor pamięci	1 MB
9	Inne	Z urządzeniem muszą być dostarczone: - wkładki SFP+ Multimode 10GB iSCSI minimum 6 szt. - wkładki SFP+ Singlemode 10GB iSCSI minimum 2 szt. - kable światłowodowe LC/LC o długości 3 metrów minimum 8 szt. (6 szt. Multimode, 2 szt Singlemode) Wkładki muszą być tego samego producenta co switch. Gwarancja minimum 3 lata

5) Firewall - 1 sztuka

L.p.	**Element konfiguracji**	**Wymagania minimalne**
1	Redundancja, monitoring i wykrywanie awarii	• 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. • Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. • Monitoring stanu realizowanych połączeń VPN. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
2	Interfejsy, Dyski	• System realizujący funkcję Firewall musi dysponować minimum 20 portami Gigabit Ethernet RJ-45, 2 gniazdami SFP 1 Gbps. • System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

		• W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. • System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB.
3	Parametry wydajnościowe	• W zakresie Firewall'a obsługa nie mniej niż 1,8 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę. • Przepustowość Stateful Firewall: nie mniej niż 7 Gbps dla pakietów 512 B. • Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 800 Mbps. • Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA1: nie mniej niż 4 Gbps. • Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 1,9 Gbps. • Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps. • Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem AES256-SHA1) dla ruchu http – minimum 300 Mbps.
4	Funkcje Systemu Bezpieczeństwa	• Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. • Kontrola Aplikacji. • Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. • Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. • Ochrona przed atakami - Intrusion Prevention

		System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. • Zarządzanie pasmem (QoS, Traffic shaping). • Analiza ruchu szyfrowanego protokołem SSL oraz SSH. • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). • 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.
5	Polityki, Firewall	• System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW. • Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. • 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. • W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
6	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 Diffiego-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. 3. Dla modułów: IPSec VPN oraz SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. Klient VPN musi umożliwiać weryfikację stanu bezpieczeństwa stacji zdalnej. 4. Rozwiązanie powinno zapewniać funkcjonalność VTEP (VXLAN Tunnel End Point)

7	Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego • Policy Based Routingu • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
8	Zarządzanie pasmem	• System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. • Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. • System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
9	Kontrola Antywirusowa	• Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). • System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. • Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
10	Ochrona przed atakami	• Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie

		anomalii w protokołach sieciowych. • Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. • System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. • 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.
11	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 2800 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, Botnet. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
12	Kontrola WWW	• Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów

		URL pogrupowanych w kategorie tematyczne. • W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware, phishing, spam, Dynamic DNS, proxy avoidance. • Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. • Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. • 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. • Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
13	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.

18	Zarządzanie	• 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. • Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. • Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. • System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. • System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. • System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
14	Logowanie	• System musi mieć możliwość logowania 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. • W ramach logowania system 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. • Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. • Musi istnieć możliwość logowania do serwera SYSLOG.
15	Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: • ICSA lub EAL4 dla funkcji Firewall • ICSA lub NSS Labs dla funkcji IPS • ICSA dla funkcji: SSL VPN, IPSec VPN
16	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, Antyspam, Web Filtering na okres 5 lat
17	Gwarancja oraz wsparcie	• Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 5 lat, 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 8x5.

6) UPS - 1 sztuka

L.p.	Element konfiguracji	Wymagania minimalne
1	Moc wyjściowa	3000VA / 2800W
2	Typ obudowy	Rack 19” 3U
3	Praca sieciowa	Napięcie wejściowe od 160-280 V Częstotliwość napięcia wejściowego 45-55 Hz tolerancja +/- 2 Hz Czas przełączania nie więcej niż 4 ms
4	Praca bateryjna	Napięcie wyjściowe 230V +/- 5% Częstotliwość napięcia wyjściowego 50 Hz

		tolerancja +/- 1 Hz Czas przełączania UPS / sieć 0 ms Zabezpieczenie przeciwzwarciowe oraz przeciążeniowe Czas ładowania nie dłużej niż 3,5 h Czas podtrzymania przy obciążeniu 80% nie mniej niż 7 minut
5	Wyposażenie	Ilość gniazd wyjściowych – min. 8 szt. Typ gniazd wyjściowych - IEC 320 C13 Filtr sieci LAN Bezpiecznik automatyczny chroniący przed prądem przetężeniowym
6	Gwarancja	Minimum 3 lata

7) Backup przenośny – 1 sztuka

L.p.	Element konfiguracji	Wymagania minimalne
1.	Urządzenie do backupu	Stacja dokująca dla nośników RDX (wymiennej pamięci dyskowej) z interfejsem USB 3.0 nie wymagająca dodatkowego źródła zasilania.
2.	Nośnik	Nośnik RDX o pojemności minimum 4 TB bez kompresji W ilości 3 szt.
3.	Gwarancja	Minimum 3 lata

8) Oprogramowanie do backupu – Licencja na 2 gniazda CPU

L.p.	Komponent	Minimalne wymagania
1	**Wymagania ogólne**	• Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2016. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej • Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. • Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. • Oprogramowanie musi zapewniać tworzenie kopii

		zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V • Oprogramowanie będzie tworzyć kopie zapasowe serwera wyposażonego w 2 procesory
2	**Całkowite koszty posiadania**	• Oprogramowanie musi być licencjonowanie w modelu "per-CPU". Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone • Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej • Oprogramowanie musi tworzyć „samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków • Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji • Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. • Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania • Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia • Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość akutalizacji pola „notatki" na wirtualnej maszynie • Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware. • Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director 5.5, 5.6, 8.0, 8.10 i archiwizować również metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD

		• Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji • Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji • Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) • Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. • Oprogramowanie musi posiadać co najmniej roczny okres wsparcia w zakresie udoskonalenia i aktualizacji.
3	**Wymagania dotyczące wykonywania kopii zapasowych**	• Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej • Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora • Oprogramowanie musi wspierać kopiowanie plików na taśmy • Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server • Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej • Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) • Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu. • Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. • Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik • Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako

		źródła do dalszej replikacji (replica seeding) • Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V • Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) • Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere • Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)
4	**Wymagania dotyczące przywracania kopii zapasowych**	• Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dla srodowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania • Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować jaką migrację swoimi mechanizmami • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure. • Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików • Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. • Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: o **Linux** ▪ ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs

		o **BSD** ▪ UFS, UFS2 o **Solaris** ▪ ZFS, UFS o **Mac** ▪ HFS, HFS+ o **Windows** ▪ NTFS, FAT, FAT32, ReFS o **Novell OES** ▪ NSS • Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. • Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. • Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, grupy oraz pozwalać na odtworzenie haseł. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. • Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia. • Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych. • Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows • Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

3. Ilekroć w niniejszym załączniku wskazano markę lub pochodzenie produktu lub urządzenia, należy przyjąć, że za każdą nazwą jest umieszczone słowo „lub równoważne”, tzn. że materiały, urządzenia, funkcjonalności oprogramowania itp. będą posiadały (charakteryzowały się) wszystkimi parametrami nie gorszymi niż opisane w w/w dokumentach. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest zobowiązany wykazać, że oferowane przez niego dostawy, usługi lub roboty budowlane spełniają wymagania określone przez Zamawiającego. Wykonawca składający tzw. ofertę równoważną ma obowiązek załączyć do oferty odpowiednie dokumenty (tj. odpowiednie dowody wykazujące równoważność oferowanych przez

Wykonawcę artykułów - zgodnie z art. 30 ust. 5 ustawy) potwierdzające równoważność artykułu oferowanego z artykułem sprecyzowanym przez Zamawiającego (oznaczonym znakiem towarowym, patentem lub pochodzeniem) karty katalogowe, opinie producentów lub inne dokumenty zawierające szczegółowy opis oferowanego przez Wykonawcę artykułu (powinny zawierać wszelkie elementy wskazane w opisie pozycji, których równoważność będzie badana przez Zamawiającego). Zamawiający zastrzega sobie możliwość wystąpienia do jednostek certyfikujących, producentów artykułów oferowanych przez Wykonawcę o wydanie karty katalogowej / opinii, w przypadku artykułów, do których pojawią się wątpliwości co do ich równoważności w stosunku do artykułu sprecyzowanego przez Zamawiającego.

4. Oferowany przez Wykonawcę sprzęt oraz oprogramowanie wskazane winno być kompatybilne z aktualnie używanym przez Zamawiającego oprogramowaniem, tj.:
   1) RADIX:
      EGW+ - wersja 1.12
      ELUD+ - wersja 3.03
      GOK+ - wersja 4.24
      MKO+ - wersja 1.09
      NDZ+ - wersja 2.06
      POGRUN+ - wersja 3.15
      POST+ - wersja 2.09
      WIP+ - wersja 3.19
   2) Windows Server 2016,
   3) Windows Server 2012 R2
   4) Microsoft Exchange Server 2016