nr zapytania ofertowego 3/KON/A017/2022

Załącznik nr 4 do Warunków

Specyfikacja nr 4

System nr 4 – PLATFORMA ZDALNEGO NAUCZANIA – INFRASTRUKTURA SPRZĘTOWA – zakup infrastruktury niezbędnej do uruchomienia platformy zdalnego nauczania.

nr zapytania ofertowego 3/KON/A017/2022

Zakup infrastruktury sprzętowej niezbędnej do uruchomienia Platformy Zdalnego Nauczania

W ramach projektu Zamawiający planuje zakup i utrzymanie własnej chmury serwerowej dedykowanej do Platformy Zdalnego Nauczania złożonej z 3 fizycznych serwerów oraz macierzy o dużej pojemności. Poprzez zastosowanie tak zwanej wirtualizacji zostanie tam zainstalowane zwirtualizowane serwerów pełniące różnorakie funkcje. W miarę potrzeb będzie można szybko zwiększać zasoby takich serwerów sprawiając, że będą mogły obsłużyć zwiększone potrzeby elastycznie reagując na sytuację. W celu zapewnienia bezpieczeństwa zgromadzonych tam danych zostaną zastosowane systemy backupu i archiwizacji danych, które pozwolą szybko i skutecznie odzyskać dane w przypadku ewentualnej awarii jednego z systemów. Dodatkowo planuje się również zakup urządzeń związanych z bezpieczeństwem systemów informatycznych.

Planowany zakres dostaw sprzętowych:

1. serwery wraz z systemem wirtualizacji 3 szt.
2. macierz 1 szt.
3. system archiwizacji danych 1 szt.
4. firewall 2 szt.

1. Wymagania dla Zakupu Infrastruktury Sprzętowej:

1.1. Serwer – 3 sztuki

W ramach dostaw serwerów należy dostarczyć:

- serwery komputerowe (hardware) – 3 sztuki
- przełączniki SAN (hardware) – 2 sztuki
- przełąniczki LAN (hardware) – 2 sztuki
- system wirtualizacji serwerów (software) – licencja na 3 dostarczone serwery
- system operacyjny na serwery (software) – licencja na 3 dostarczone serwery

Serwer komputerowy – 3 sztuki – parametry minimalne dla 1 sztuki

Element konfiguracji	**Wymagania minimalne**
Obudowa	Maksymalnie 1U RACK 19 cali wraz z szynami montażowymi. Serwer wyposażony w zamykany, zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków Serwer wyposażony w czujnik otwarcia obudowy współpracującego z BIOS/UEFI. Serwer wyposażony w moduł TPM 2.0.
Procesor	Jeden procesor 16-rdzeniowy, x86 - 64 bity, Intel Xeon 4314 (2.4GHz/16-core/135W) lub równoważne procesory 16-rdzeniowe, osiągające w testach SPECrate2017_int_base powyżej 134 punktów w konfiguracji

	dwuprocesorowej. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org. Płyta główna wspierająca zastosowanie procesorów od 4 do 40 rdzeniowych, mocy do min. 270W i taktowaniu CPU do min. 3.4GHz.
Liczba procesorów	Min. 1 procesor
Pamięć operacyjna	256 GB RDIMM DDR4 3200 MT/s w modułach o pojemności minimum 32GB każdy. Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację minimum 8TB pamięci RAM. Płyta główna z fabrycznym oznaczeniem logo producenta (dopuszcza się logo producenta na module zarządzania trwale zintegrowanym na płycie głównej). Obsługa zabezpieczeń: Advanced ECC, Memory Mirror, Online Spare (Rank Sparing).
Sloty rozszerzeń	Serwer musi być wyposażony w: - 2 aktywne gniazda PCI-Express generacji 4, każde gniazdo x16 i pozwalać na rozbudowę do 3 aktywnych gniazd PCI-Express generacji 4, każde gniazdo x16 (szybkość slotu – bus width) Serwer musi mieć dodatkowo dedykowane dwa sloty PCI-Express: - na kontroler dyskowy; - na kartę sieciową niezajmującą slotów PCI-Express.
Zasoby dyskowe	Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD/NVMe U.3, 2,5”. Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 32GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. Serwer wyposażony w 2 dyski 240GB SSD SATA Read Intensive.
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 16 linii SAS/SATA/NVMe oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie

nr zapytania ofertowego 3/KON/A017/2022

Interfejsy sieciowe	Serwer musi być wyposażony w: - 1 dwuportowa karta 10Gb Ethernet SFP+, do kart należy dołączyć 2 sztuki wkładek 10Gb SFP+ SR; - 1 dwuportowa karta 10Gb Ethernet (RJ-45) – umieszczona w dedykowanym slocie na kartę sieciowa niezajmującą slotów PCI-Express opisana w „Sloty roszerzeń”. - 1 dwuportowa karta 16GB fibre channel
Karta graficzna	Zintegrowana karta graficzna
Porty	5x USB 3.0 (w tym 2 porty wewnętrzne) 1x VGA 1x port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45. Nie dopuszcza się stosowania kart PCI. Możliwość rozbudowy o: - dodatkowy port DisplayPort dostępny z przodu serwera bez stosowania jakichkolwiek przejściówek;
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 800W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Karta/moduł zarządzający i system zarządzania	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia mininmalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl)

	- poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power caping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającejj (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2019 lub nowszy Red Hat Enterprise Linux (RHEL) 7.9 lub nowszy SUSE Linux Enterprise Server (SLES) 12 SP5 lub nowszy VMware ESXi 6.7 lub nowszy

Wsparcie techniczne	3-letnia gwarancja producenta w miejscu instalacji. Czas reakcji to kolejny dzień roboczy. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera.
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.

Przełącznik SAN – 2 sztuki

W ramach postepowania należy dokonać rozbudowy 2 szt. posiadanych przełączników FC (Brocade 16Gb/16 SAN Switch for HPE BladeSystem c-Class, part numer: C8S45A) umieszczonych w obudowie blade C7000. Rozbudowa ma polegać na aktywacji w każdym przełączniku kolejnych 6 portów FC po przez zakup licencji oraz dodatkowych wkładek FC 16GB SFP. Rozbudowa ma być objęta wsparciem 3 letnim z reakcją w ciągu następnego dnia roboczego od zgłoszenia. Poniżej lista pn do rozbudowy:

Szt.	Numer katalogowy	Nazwa urządzenia/usługi
2	T5517AAE	Brocade 8/16Gb Embedded FC Switch 6-port Upgrade E-LTU
12	QK724A	HPE B-series 16Gb SFP+ Short Wave Transceiver
1	HU4B2A3	HPE 3Y Tech Care Basic Service

Oraz dostarczyć przełącznik SAN (łącznie 2 szt.) o minimalnych wymaganiach:

L.p.	Cecha	Wymagania minimalne
1.	Rodzaj przełącznika	Przełącznik musi być wykonany w technologii FC minimum 32 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gb/s w zależności od rodzaju zastosowanych wkładek SFP+.
2.	Wydajność	Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji, gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 32 Gb/s.

		Całkowita przepustowość przełącznika FC musi wynosić minimum 768 Gb/s end-to-end. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900 ns.
3.	Ilość portów	Przełącznik FC musi posiadać minimum 24 aktywnych portów. Przełącznik FC musi być dostarczony wraz z wkładkami 16Gb/s SFP+ SW w liczbie 24 sztuki.
4.	Rodzaj obsługiwanych portów	Co najmniej: E, F, M, S, D Port.
6.	Typ obudowy	Przełącznik FC musi być przystosowany do montażu w szafie typu rack 19”, o wysokości maksymalnie 1U. Przełącznik musi być wyposażony w akcesoria umożliwiające montaż w szafie.
7.	Zasilanie	Urządzenie musi posiadać wbudowany zasilacz z 4 aktywnie działającymi wentylatorami. Do poprawnego działania urządzenia wymagane powinny być minimum dwa działające wentylatory.
8.	Agregacja połączeń	Przełącznik FC musi być musi obsługiwać mechanizm agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu ISL. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC, a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. Jeżeli funkcjonalność ta wymaga odrębnej licencji, licencja jest wymagana.
11.	Zoning	Przełącznik FC musi realizować sprzętową obsługę zoningu na podstawie portów i adresów WWN.
12.	Aktualizacja przełącznika	Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wyższą wersję jak i niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC.
13.	Bezpieczeństwo	Przełącznik FC musi wspierać mechanizmy zwiększające poziom bezpieczeństwa: • uwierzytelnianie przełączników w sieci fabric za pomocą protokołów DH-CHAP i FCAP; • mechanizm tzw. Port Binding,

		• uwierzytelnianie urządzeń końcowych w sieci fabric za pomocą protokołu DH-CHAP; • szyfrowanie połączenia z konsolą administracyjną (wsparcie dla SSHv2); • definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control); • definiowane kont administratorów w środowisku RADIUS i LDAP w MS Active Directory, Open LDAP, TACACS+; • szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS; • obsługa minimum SNMP v3; • IP Filter dla portu administracyjnego przełącznika; • wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP; wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP.
14.	Sposób zarządzania	Przełącznik FC musi mieć możliwość konfiguracji przez polecenia tekstowe w interfejsie znakowym konsoli terminala oraz przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie. Interfejs graficzny oprogramowanie musi umożliwiać podstawową konfigurację i zarządzanie przełącznikiem.
15.	Diagnostyka i analiza ruchu FC	Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC: • logowanie zdarzeń poprzez mechanizm „syslog”, • ciągłe monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric • port diagnostyczny tzw. D_port, który umożliwia wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami;

		• FCping; • FC traceroute; • kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika, testowe obciążenie połączenia pełną przepustowością 32Gb/s oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością do 5m dla wkładek SFP 32Gb/s (testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric); • mechanizm sprzętowego generatora ruchu umożliwiającego symulowanie komunikacji w wielodomenowych sieciach SAN bez konieczności angażowania fizycznych urządzeń takich jak serwery lub macierze dyskowe (jeżeli funkcjonalność ta wymaga dodatkowej licencji, dostarczenie jej nie jest wymagane); • mechanizm umożliwiający pomiar opóźnień operacji zapisu i odczytu na wybranych portach dla wskazanych przepływów danych (jeżeli funkcjonalność ta wymaga dodatkowej licencji, dostarczenie jej nie jest wymagane);
16.	Dostęp	Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, port szeregowy, inband IP-over-FC oraz USB.
17.	Wsparcie SMI-S	Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S
18.	Logiczne przełączniki	W przełączniku FC musi istnieć możliwość wydzielenia logicznych, izolowanych od siebie przełączników. Każdy z logicznych przełączników musi mieć własny Domain ID, własne usługi fabric (tzw. fabric services), niezależną bazę zoningu oraz możliwość przypisania dedykowanego administratora.
19.	Kategoryzacja ruchu	Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas

		priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu.
20.	Obsługa NVMe	Przełącznik FC musi zapewniać obsługę protokołu NVMe over FC.
21.	Mechanizmy QoS	Przełącznik FC musi umożliwiać wprowadzenie ograniczenia prędkości dla danych wchodzących dla dowolnego portu lub portów. Musi być możliwość określenia wartości limitu przepustowości danych wchodzących niższej niż wynegocjowana prędkość portu.
22.	NPIV	Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
23.	Kompatybilność	Pełna kompatybilność z aktualnie posiadanymi przełącznikami Zamawiającego: • 2 przełączniki FC: Brocade 16Gb/16 SAN Switch for HPE BladeSystem c-Class
24.	Dodatkowe wymagania	Wszystkie opisane funkcje przełącznika mają być dostępne w urządzeniu na dzień składania ofert i być udokumentowane w publicznie dostępnej dokumentacji na stronach internetowych producenta. Przełącznik musi spełniać wszystkie minimalne wymagania. Jeśli funkcjonalności te wymagają dodatkowych licencji, licencje te nie są wymagane.

Przełacznik LAN – 2 szt.:

Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

- Ilość portów 24 porty 10GBaseT, 24 x SFP+
- Chłodzenie od przodu do tyłu obudowy
- Możliwość instalacji redundantnego zasilacza
- Tablica MAC min. 128K
- Tablica ARP/NDP min. 8K
- Bufor 56Mb
- MTBF min. 133176 godzin
- Wydajność min. 714 Mp/s
- Przepustowość min. 960 Gb/s
- Port USB
- Port miniUSB
- Port zarządzania Out-of-band;
- Port konsolowy RJ45 RS232

- Web GUI
- HTTPs
- CLI
- Telnet
- SSH
- SNMP
- MIB RSPAN
- Radius
- TACACS+
- DiffServ
- Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
- IPv4/IPv6 Multicast filtering
- IGMPv3 MLDv2 Snooping
- ASM & SSM
- IGMPv1,v2 Querier
- Auto-VoIP
- Auto-iSCSI
- Policy-based routing (PBR)
- LLDP-MED
- Spanning Tree
- Green Ethernet
- STP
- MTP
- RSTP
- PV(R)STP
- BPDU/STRG Root Guard
- EEE (802.3az)
- GVRP/GMRP
- Q in Q,
- Private VLAN
- DOT1X
- MAB
- Captive Portal
- DHCP Snooping
- Dynamic ARP
- Inspection
- IP Source Guard
- CPU min 800 Mhz
- Min 1GB RAM
- Min 256MB Flash
- Min ilość obsługiwanych VLAN 4K
- DHCP Server min 2K rezerwacji
- sFlow
- Minimalna ilość obsługiwanych przełączników w stosie: 8
- Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s
- Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
- Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh

nr zapytania ofertowego 3/KON/A017/2022

- Non-stop forwarding (NSF)
- Distributed Link Aggregation (LAGs across the stack)
- Ilość interfejsów IP 128
- Double VLAN Tagging (QoQ)
- PIM-DM (Multicast Routing - dense mode)
- PIM-DM (IPv6)
- PIM-SM (Multicast Routing - sparse mode)
- PIM-SM (IPv6)
- RIPv1
- RIPv2
- OSPFv2
- RFC 2328
- RFC 1583
- OSPFv3
- OSPFv2 min. sąsiadów 400
- OSPFv3 min. sąsiadów 400
- OSPFv3 min. sąsiadów na interfejs 100
- UDLD
- LLPF
- DHCPv6 Snooping
- wysyłanie alertów na email
- MMRP
- Ilość ACL min. 100
- Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu
- Zasilacz z certyfikatem 80+
- CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014,
- Class A, EN 61000-3-3:2013, EN 55024:2010
- VCCI : VCCI-CISPR 32:2016, Class A
- RCM: AS/NZS CISPR 32:2013 Class A
- FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014
- ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014
- BSMI: CNS 13438 Class A

System wirtualizacji serwerów – licencja na 3 dostarczane serwery

Należy dostarczyć licencje na trzy dostarczone serwery obejmujące wszystkie core procesorów.

Wymaga się dostarczenia licencji na oprogramowanie w najnowszej wersji obecnie dostępnej na rynku.

Dopuszcza się aby system wirtualizacji dostarczony był w ramach dostarczanego serwerowego systemu operacyjnego.

System wirtualizacji musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.

nr zapytania ofertowego 3/KON/A017/2022

3. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
6. Uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
   - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
   - Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
   - Obsługi 4-KB sektorów dysków
   - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
   - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
   - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

System operacyjny – licencja na 3 dostarczane serwery

Należy dostarczyć licencje na trzy dostarczone serwery obejmujące wszystkie core procesorów.

Wymaga się dostarczenia licencji na oprogramowanie w najnowszej wersji obecnie dostępnej na rynku.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.

7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
    a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
    b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

nr zapytania ofertowego 3/KON/A017/2022

19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c. Zdalna dystrybucja oprogramowania na stacje robocze.
    d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        i. Dystrybucję certyfikatów poprzez http
        ii. Konsolidację CA dla wielu lasów domeny,

iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f. Szyfrowanie plików i folderów.

g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

h. h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

i. Serwis udostępniania stron WWW.

j. Wsparcie dla protokołu IP w wersji 6 (IPv6),

k. Wsparcie dla algorytmów Suite B (RFC 4869),

l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

iii. Obsługi 4-KB sektorów dysków

iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

1.2. Macierz – 1 sztuka

L.p.	Cecha	Wymagania minimalne
1.	Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”. Macierz wyposażona w zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków
2.	Przestrzeń dyskowa	Macierz musi być wyposażona w minimum 6 dysków SAS o pojemności minimum 1,8 TB. Macierz musi być wyposażona w minimum 2 dysków SAS SSD o pojemności minimum 1,92 TB Read-Intensive.
3.	Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 96 dysków twardych.
4.	Obsługa dysków	Macierz musi obsługiwać dyski SSD, SAS i NL SAS. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. Komunikacja z dyskami 12Gb SAS.
5.	Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5, RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych (tzw. wide-striping). Macierz musi umożliwiać utworzenie pojedynczej grupy RAID zabezpieczonej podwójną parzystością stworzonej ze 128 dysków. Konfiguracja takiej grupy RAID musi umożliwiać zmianę rozmiaru takie grupy poprzez dodawanie i odejmowanie pojedynczych dysków w trybie online bez konieczności przerywania dostępu do danych.
6.	Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe w sieci FC 16Gb. Kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów FC i LAN.
7.	Pamięć cache	Każdy kontroler macierzowy musi być wyposażony w minimum 12GB pamięci Cache, 24 GB sumarycznie w

		macierzy. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
8.	Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.
9.	Interfejsy do hostów	Macierz musi posiadać, co najmniej 4 portów FC 16Gb obsadzone wkładkami SFP SW 16 Gb.
10.	Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. Wymagana możliwość autentykacji poprzez LDAP oraz funkcjonalność role-based access control. Wymaga się możliwości definiowania przynajmniej następujących poziomów dostępu do macierzy: • administrator – pełen dostęp, • monitor – możliwość odczytu konfiguracji.
11.	Kreator konfiguracji	System zarzadzania powinien posiadać funkcjonalność kreatora konfiguracji uruchamianego w przypadku braku zdefiniowanych pul dyskowych i wolumenów, w przypadku braku zdefiniowanych powiadomień oraz braku wykrycia jakichkolwiek zadań wykonywanych na macierzy.
12.	Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Możliwość tworzenia wolumenów logicznych o pojemności maksymalnej co najmniej 140TB. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.
13.	Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie Thin Provisioning.

		Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
14.	Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
15.	Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
16.	Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 2 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

17.	Zdalna replikacja danych	Macierz w przyszłości musi umożliwiać w asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy.
18.	Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux, VMware. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
19.	Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
20.	Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.

1.3. System Archiwizacji Danych – 1 sztuka

nr zapytania ofertowego 3/KON/A017/2022
Na System Archiwizacji danych składają się:

- półka dyskowa do archiwizacji danych (hardware)– 1 sztuka

- oprogramowanie do archiwizacji danych (software) – 1 sztuka

Półka dyskowa do archiwizacji danych – 1 sztuka – wymagania minimalne dla jednej sztuki

W ramach postepowania należy dostarczyć półkę dyskową w celu podłączenia do posiadanego serwera DL360 Gen10:

Obudowa	Wysokość 2U z możliwością zainstalowania 12 dysków SAS/SATA 3,5”
Dyski Twarde	Wraz z obudową należy dostarczyć 12 dysków 8TB SAS12G, każdy dysk hot-swap
Kable	Wraz z półką należy dostarczyć 2 szt. kabli HPE External 2.0m (6ft) Mini-SAS HD 4x to Mini-SAS HD 4x Cable w celu podłączenia do posiadanego serwera DL360 Gen10
Kontroler RAID	Wraz z półka dyskową należy dostarczyć kontroler sprzętowy zewnętrzny z min. 2GB, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60 do podłączenia dostarczanej półki dyskowej do serwera DL360 Gen10. Kontrolef ma być kompatybilny z posiadanym serwerem oraz dostarczaną półką dyskową

Oprogramowanie do archiwizacji danych – 1 sztuka – wymagania minimalne dla jednej sztuki

Wymagania ogólne

1. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
2. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej

3. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
4. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
5. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Całkowite koszty posiadania

1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
2. Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
3. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
4. 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
5. 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.
6. Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
7. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
8. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
9. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
10. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
11. 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
12. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
13. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
14. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Wymagania RPO

nr zapytania ofertowego 3/KON/A017/2022

1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
2. Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
4. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
5. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
6. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
7. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
8. Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
9. Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
10. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
11. Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)
12. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
13. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
14. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
15. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

<u>Wymagania RTO</u>

1. Oprogramowanie musi umożliwiać jednoczesne 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 dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.

nr zapytania ofertowego 3/KON/A017/2022

2. Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
3. 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 taką migrację swoimi mechanizmami
4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
5. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
7. 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
8. 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.
9. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
    - Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
    - BSD: UFS, UFS2
    - Solaris: ZFS, UFS
    - Mac: HFS, HFS+
    - Windows: NTFS, FAT, FAT32, ReFS
    - Novell OES: NSS
10. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
11. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
12. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
13. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
14. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
15. Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
16. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
17. Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
18. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych

nr zapytania ofertowego 3/KON/A017/2022

19. Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
20. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
21. Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
22. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka

1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
2. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
3. Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
4. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
5. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

1.4. Firewall – 2 sztuki

Dostarczone urządzenia typu firewall (2 sztuki) mają pracować w układzie klastra HA zapewniającego wysoka niezawodność rozwiązania.

Klaster HA (złożony z 2 sztuk urządzeń) składa się z następujących elementów:

Funkcje modułu Firewall

1. Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
2. Możliwość uruchomienia w formie klastra wysokiej dostępności (HA) - co najmniej Active-Passive.
3. Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
4. Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.

5. Musi obsługiwać Multicast routing.
6. Musi obsługiwać Policy Based routing.
7. Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.
8. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
9. Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.
10. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
11. Musi obsługiwać Dynamic DNS.
12. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
13. Musi obsługiwać translację portów: PAT.
14. Musi obsługiwać IPSec NAT traversal.
15. Musi obsługiwać mechanizm Policy Based NAT.
16. Musi obsługiwać VLAN 802.1Q.
17. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
18. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
19. Musi mieć możliwość obsługi zapasowego łącza typu LTE poprzez podłączenie zewnętrznego modemu USB.
20. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
21. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.
22. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza.
23. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
24. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
25. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.
26. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.
27. Urządzenie musi posiadać co najmniej 4 mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Active Directory.

nr zapytania ofertowego 3/KON/A017/2022

28. Co najmniej dwie metody transparentnej autoryzacji nie wymagają instalacji dedykowanego agenta na stacjach roboczych użytkowników.
29. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.
30. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
31. Musi dostarczać mechanizmów identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
32. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
33. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
34. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.
35. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
36. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.
37. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.
38. Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
39. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.
40. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.

Dostarczony system bezpieczeństwa musi zapewniać:

1. Ochronę z wykorzystaniem mechanizmów IPS.
2. Ochronę antywirusową.
3. Ochronę przed nieznanymi zagrożeniami.
4. Ochronę przed phishingiem.
5. Ochronę przed niechcianą pocztą.
6. Kontrolę wykorzystywanych aplikacji.
7. Możliwość filtrowania URL.

nr zapytania ofertowego 3/KON/A017/2022

Parametry fizyczne systemu Firewall:

Element systemu pełniący funkcję Firewall musi dysponować :

- 8 portami 1Gb RJ45.
- 2 portami 10Gb SFP+.
- System powinien umożliwiać rozbudowę o dodatkowe porty: 4 x SFP lub

2 x SFP+ lub 4 x RJ45 PoE+.

- Minimum 8 GB pamięci RAM.
- Minimum 2 porty USB 3.0.
- Minimum jeden port typu Console.
- System musi być wyposażony w 2 zasilacze AC.
- Minimalna temperatura pracy urządzenia od 0 do 40 stopni Celsjusza.

Parametry wydajnościowe systemu:

- Przepustowość Firewall minimum: 20 Gbps.
- Przepustowość IPSec VPN nie mniejsza niż: 6.84 Gbps.
- Przepustowość skanowania antywirusowego nie mniejsza niż: 5 Gbps.
- Przepustowość w ramach ochrony przed atakami nie mniejsza niż: 4.6 Gbps.
- Przepustowość systemu z włączonymi mechanizmami skanowania antywirusowego, ochrony przed atakami, kontroli aplikacji minimum: 3.3 Gbps.
- Obsługa nie mniej niż: 500 tuneli IPSec site-to-site.
- Obsługa nie mniej niż: 500 tuneli client-to-site.
- Obsługa nie mniej niż: 6.000.000 jednoczesnych połączeń.
- Obsługa nie mniej niż: 132.000 nowych połączeń na sekundę.
- W ramach Firewall system musi obsługiwać minimum: 750 sieci VLAN.

W ramach ochrony przed atakami system musi zapewniać:

1. Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 4500 definicji sygnatur.
2. Automatyczne blokowanie znanych źródeł ataków.
3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.

nr zapytania ofertowego 3/KON/A017/2022

4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).

5. Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer OverFlow, Remote File Inclusions.

6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.

W ramach kontroli antywirusowej system musi zapewniać:

1. Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie lub system musi posiadać mechanizmy integracji z drugim zewnętrznym skanerem działającym lokalnie. W przypadku skanera zewnętrznego koniecznym jest dostarczenie pełnej dokumentacji przykładowego systemu oraz wykazanie w testach poprawności działania takiej integracji z zewnętrznym skanerem lokalnym.

2. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.

3. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.

4. Możliwość skanowania plików o rozmiarze co najmniej 20MB.

5. Możliwość zdefiniowania rozmiaru skanowanego pliku.

6. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.

7. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.

8. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.

9. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.

W ramach ochrony przed nieznanymi zagrożeniami system musi zapewniać:

1. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję analizy behawioralnej w oparciu o platformę typu sandbox, w tym co najmniej:

- W tym zakresie system musi pracować w trybie lokalnym lub z wykorzystaniem mechanizmów chmury (w granicach Unii Europejskiej).
- Analizę plików pobieranych przez HTTP/HTTPS i przesyłanych pocztą elektroniczną (SMTP, POP3, IMAP) oraz plików pobieranych za pomocą protokołu FTP.
- Ogólne oszacowanie poziomu ryzyka dla analizowanych plików i określanie różnego rodzaju akcji na ich podstawie.
- Kwarantannę podejrzanych plików co najmniej dla protokołu SMTP.

- Możliwość blokowania wiadomości e-mail przesyłanej protokołem SMTP zawierającej podejrzane załączniki do czasu zakończenia ich analizy.
- Możliwość analizy plików o rozmiarze co najmniej 10MB.
- Brak ograniczeń co do ilości analizowanych plików.

W ramach ochrony przed phishingiem system musi zapewniać:

1. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję ochrony przed phishingiem, w tym co najmniej:

- Możliwość blokowania dostępu do spreparowanych stron.
- Ochronę przed phishingiem nie zależnie od typu połączenia, protokołu, portu.
- Możliwość tworzenia białych/czarnych list domen, do których połączenia będą filtrowanie.
- Notyfikację użytkownika, którego dotyczy zdarzenie - niezależnie od logów i raportów.
- Kontrolę zapytań DNS.

W ramach kontroli antyspamowej system musi zapewniać:

1. Analizę wiadomości pocztowych w oparciu o technologię Recurrent Pattern Detection.
2. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.
3. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
4. Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
5. Możliwość tworzenia białych/czarnych list, w oparciu o które system zezwala lub odmawia wysyłania wiadomości e-mail dla określonych nadawców i odbiorców.
6. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.

W ramach filtrowania zawartości URL system musi zapewniać:

1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
2. Baza filtra url powinna zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
3. Odpytywanie bazy on-line w czasie rzeczywistym.
4. Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym dlaczego dostęp do strony www został zablokowany.
5. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.

6. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
7. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.
8. Możliwość określania reputacji adresu URL i na podstawie reputacji podejmowanie określonych akcji.
9. Możliwość filtrowania treści w oparciu o typy MIME.
10. Możliwość blokowania plików cookies dla określonych domen.
11. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
12. Analizę treści dla protokołu https.
13. Wyłączenie inspekcji https dla wybranych kategorii stron www.

W ramach kontroli aplikacyjnej system musi zapewniać:

1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
2. Ilość rozpoznawanych aplikacji: nie mniej niż 1000, podzielonych na kategorie.
3. W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
4. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.
5. Możliwość ograniczania wykorzystywanej przepustowości aplikacji lub kategorii aplikacji.

Wymagane funkcje VPN systemu:

1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
5. Obsługa Dead Peer Detection (DPD).
6. Wsparcie dla IKEv1 i IKEv2.
7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.

nr zapytania ofertowego 3/KON/A017/2022

10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.
12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.
13. Musi umożliwiać uruchomienie portalu SSL VPN, który umożliwia autoryzację w oparciu o protokoły RADIUS, LDAP, Active Directory, lokalną bazę użytkowników.
14. Portal SSL VPN musi zapewniać wsparcie dla protokołów: SSH, RDP, HTTP.
15. Portal SSL VPN musi wspierać funkcjonalność Single-Sign-On dla aplikacji webowych w oparciu o protokół SAML.

Zarządzanie

1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.
8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.

Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania:

1. Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
2. Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
3. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online

4. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według zdefiniowanego harmonogramu.
5. Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
6. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję porównywania różnych wersji konfiguracji. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
7. Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
8. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
9. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
10. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
11. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
12. Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
13. Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
14. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
15. Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
16. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
17. System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.
18. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
19. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
20. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
21. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
22. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
23. Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.

Licencje i wsparcie techniczne

nr zapytania ofertowego 3/KON/A017/2022

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

   - Ochrona przed atakami (IPS), Kontrola aplikacji, Web Filtering, Antyspam, Antywirus, Bazy reputacyjne adresów, Rozpoznawanie urządzeń pracujących w sieci, Ochrona przed nieznanymi zagrożeniami, Ochrona przed phishingiem, – na okres 3 lat.

2. System musi być objęty serwisem gwarancyjnym producenta przez okres 3 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 24x7 (świadczone telefonicznie lub poprzez portal).

Gwarancja na ww. sprzęt i oprogramowanie obejmuje:

1. Gwarancja na dostarczony sprzęt wynosi minimum 36 miesięcy od momentu podpisania bezusterkowego protokołu odbioru realizowane w miejscu instalacji sprzętu od poniedziałku do piątku w godzinach pracy Uczelni
2. Gwarancja na dostarczone oprogramowanie wynosi minimum 36 miesięcy od momentu podpisania bezusterkowego protokołu odbioru
3. Zamawiający musi mieć możliwość samodzielnego kontaktu z serwisem świadczonym przez producenta sprzętu, oraz aktualizacji oprogramowania.
4. Przełączniki SAN, serwery oraz półka dyskowa muszą pochodzić od jednego producenta i objęte jednolitym serwisem producenta
5. Możliwość zgłoszenia awarii przez 24 godziny na dobę.
6. W razie wystąpienia awarii, rozumianej jako nagłe i nieprzewidziane uszkodzenie programu/ów lub sprzętu uniemożliwiające jego użycie – czas reakcji do 4 godziny robocze, czas naprawy do 20 godzin roboczych;
7. W razie wystąpienia błędu w oprogramowaniu/ach, rozumianego jako brak poprawnego prawidłowego działania programu lub jego elementu/funkcji umożliwiającego jednak pracę przez zastosowanie tzw. obejścia - czas reakcji do 16 godzin roboczych, czas naprawy do 5 dni roboczych;
8. W razie wystąpienia usterki, rozumianej jako „kosmetyczna” wada techniczna obniżająca jakość działania programu/ów - czas reakcji do16 godzin roboczych, czas naprawy 7 dni roboczych;

   gdzie:

   czas reakcji - to czas, jaki upłynie od przyjęcia zgłoszenia wady do potwierdzenia rozpoczęcia analizy zgłoszenia przez Wykonawcę;

   czas naprawy - to czas jaki upłynie od potwierdzenia przyjęcia zgłoszenia do jego całkowitego rozwiązania, przy czym do czasu naprawy zalicza się wyłącznie czas pracy Wykonawcy.

9. W okresie gwarancji Zamawiający ma prawo do otrzymywania bezpłatnych poprawek oraz aktualizacji wersji dostarczonego oprogramowania.