**Zał. nr 8 do SWZ**

**Opis przedmiotu zamówienia do postępowania pn.**

**Rozbudowa systemu backupu zapewniająca spełnienie warunku stworzenia zapasowej kopii w trybie offline oraz wykonanie audytu**

Zamawiający podzielił zamówienie na dwie niżej wymienione części:

Część A – Rozbudowa systemu backupu zapewniająca spełnienie warunku stworzenia zapasowej kopii w trybie offline

Część B – Audyt weryfikujący podniesienie poziomu bezpieczeństwa

**CZĘŚĆ A – Rozbudowa systemu backupu zapewniająca spełnienie warunku stworzenia zapasowej kopii w trybie offline.**

Założeniem jest rozszerzenie obecnego rozwiązania backupu opartego o oprogramowanie Veeam. Obecne rozwiązanie oparte jest o serwer backupu na którym kopie zapasowe przechowywane są na dyskach lokalnych serwera. Proponowane rozwiązanie ma za zadanie zwiększyć retencję przechowywania kopii, zwiększyć bezpieczeństwo kopii poprzez przeniesienie na rozwiązanie macierzowe oraz zapewnić repozytorium backupu trybu offline.

Proponowane rozwiązanie składać się ma z dwóch macierzy blokowych z interfejsami 10Gb SFP+ połączonymi przełącznikami zawierającymi 24 porty 10Gb SFP+.

Jedna z dwóch macierzy ma rozszerzyć i zwiększyć wiarygodność podstawowego repozytorium backupu. Druga z macierzy ma służyć jako kolejna kopia zapasowa, która w ściśle określonych interwałach czasowych będzie odpinana od sieci LAN co zapewnia warunek braku dostępu fizycznego.

Macierze mają posiadać symetryczne przestrzenie na kopie zapasowe i ich kolejne kopie.

1. **Wykonanie projektu technicznego przed przystąpieniem do prac**
2. **Zainstalować i skonfigurować nowe redundantne przełączniki sieciowe dla celów podłączenia serwera oraz macierzy backupu w niezależną sieć SAN.**
3. **Zapewnić mechanizm skryptowy wyłączający porty sieciowe przełączników w określonych interwałach czasowych, co oznacza cykliczne odłączanie sieci LAN od macierzy backupu w trybie offline.**
4. **Podłączyć i skonfigurować macierz backupu podstawową. Podłączenie wielościeżkowe, redundantne przez kontrolery macierzowe, z użyciem protokołu iSCSI.**
5. **Re-konfigurować repozytorium zadania backupu i replikacji na nowe repozytorium backupu.**
6. **Wykonać testy poprawności wykonywania zadań kopi i testy odzyskiwania poszczególnych VM, plików.**
7. **Podłączyć i skonfigurować macierz zapasową trybu offline. Mechanizm kolejnych kopii zapasowych może być zrealizowany z użyciem oprogramowania Veeam lub mechanizmów replikacji wolumenów pomiędzy macierzami.**
8. **Zapewnić instalację i konfigurację stacji zarządzającej dedykowanej do zarządzania macierzami kopii zapasowych. Stacja zarządzająca powinna znajdować się minimum w odrębnej sieci vLAN dedykowanej do celów zarządzających.**
9. **Stacja zarządzająca powinna być podłączona do wysuwanego urządzenia typu KVM zapewniającego jedną wspólną konsolę dla serwerów.**
10. **W ramach zadania należy również doposażyć istniejący serwer backupu firmy Fujitsu o dwuportowy interfejs sieciowy 10Gb SFP+.**
11. **Macierz dyskowa (2szt.)**

|  |  |
| --- | --- |
| **1** | **Wymagania techniczne** |
| 1.1 | Obudowa - gęstość upakowania :  a. Możliwość zainstalowania w standardowej szafie RACK 19”  b. Urządzenie musi wykorzystywać półki dyskowe wysokiej gęstości upakowania - co najmniej 24 dyski na 2U wysokości dla dysków 2,5 cala oraz półki dyskowe zawierające co najmniej 12 dysków 3,5 cala na wysokości 2U.  c. Urządzenie musi wykorzystywać półki dyskowe wysokiej gęstości umożliwiające upakowanie co najmniej 90 dysków na maksymalnej wysokości 5U. |
| 1.2 | Zarządzanie:  a. Urządzenie musi umożliwiać zarządzanie za pomocą interfejsu Ethernet.  b. Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej.  c. Funkcjonalność bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje.  d. Interfejs zarządzający GUI, CLI, oraz zapewnienie możliwości tworzenia skryptów użytkownika. |
| 1.3 | Ilość portów:  a. Wymagane jest nie mniej niż 4 porty 1Gb Ethernet Base-T oraz 8 portów 10Gb SFP+ wyposażonych w oryginalne wkładki GBIC. |
| 1.4 | Obsługa dysków:  a. musi obsługiwać dyski SAS:  - o prędkościach obrotowych 10000 obr./min. i pojemnościach 1.2TB, 1.8TB, 2.4TB;  - o prędkościach obrotowych 7200 obr./min. i pojemnościach 2TB, 4TB, 6TB, 8TB, 10TB, 12TB, 14TB, 16TB;  b. musi obsługiwać dyski SSD o pojemnościach 800 GB, 1.92 TB , 3.84 TB, 7.68 TB, 15.36 TB, 30.72 TB.  c. musi obsługiwać, co najmniej 380 dysków na parę kontrolerów z zastosowaniem dodatkowych półek. Macierz musi umożliwiać rozbudowę o pojedyncze dyski fizyczne i pojedyncze półki rozszerzeń.  d. musi umożliwiać konfigurację, która w jednym rozwiązaniu łączyć będzie półki rozszerzeń na dyski 2,5” z półkami na dyski 3,5”. |
| 1.5 | Pojemność dyskowa:  Macierz dyskowa musi być wyposażona w minimum:  11 dysków 12TB 7.2K 3.5 Inch NL HDD |
| 1.6 | Macierz musi zapewnić możliwość wymiany uszkodzonych dysków podczas pracy systemu (Hot-Swap). Macierz musi być umożliwiać stworzenie konfiguracji odpornej na awarię pojedynczego dysku oraz odporność na awarię dwóch dysków. Przestrzeń zapasowa powinna być realizowana za pomocą przestrzeni zapasowej rozmieszczonej na wszystkich dyskach w ramach grupy RAID lub w formie dysku nadmiarowego. |
| 1.7 | Obsługa pamięci Cache:  Macierz musi być wyposażona w minimum 64GB pamięci Cache, która w 95% musi być przeznaczona na obsługę operacji wejścia/wyjścia. |
| 1.8 | Wsparcie dla systemów operacyjnych:  Macierz musi wspierać następujące systemy operacyjne i wirtualizatory: MS Windows Server 2012/2012R,2016,2019 Vmware vSpere 6.x/7.x, RedHat Enterprise Linux 6.x/ 7.x. |
| **2** | **Dodatkowe wymagania i funkcjonalności** |
| 2.1 | Funkcje niezawodnościowe:  a. Wszystkie krytyczne komponenty urządzenia takie jak: kontrolery dyskowe, pamięć cache, zasilacze i wentylatory muszą być zdublowane tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu.  b. Komponenty te muszą być wymienialne w trakcie pracy macierzy.  c. Urządzenie musi cechować brak pojedynczego punktu awarii.  d. Wsparcie dla zasilania z dwóch niezależnych źródeł prądu poprzez nadmiarowe zasilacze typu Hot-Swap.  e. Wentylatory typu Hot-Swap.  f. Wbudowane co najmniej dwa kontrolery RAID.  g. Urządzenie musi posiadać pamięć typu Flash dla zapisu danych z pamięci cache na wypadek zaniku zasilania oraz system podtrzymania zasilania pozwalający na zapis danych z cache do pamięci typu Flash. |
| 2.2 | Funkcjonalności:  a. Musi istnieć funkcjonalność Cache dla procesu odczytu.  b. Musi istnieć funkcjonalność Mirrored Cache dla procesu zapisu.  c. Możliwość wyłączenia cache dla poszczególnych wolumenów.  d. Funkcjonalność partycjonowania pamięci cache.  e. Funkcjonalność separacji przestrzeni dyskowych pomiędzy różnymi podłączonymi hostami.  f. Funkcjonalność dynamicznego zwiększania i zmniejszania rozmiaru wolumenów.  g. Funkcjonalność zarządzania ilością operacji wejścia / wyjścia wykonywanych na danym wolumenie – zarządzanie musi być możliwe zarówno poprzez określenie ilości operacji I/O na sekundę jak również przepustowości określonej w MB/s.  h. Urządzenie musi obsługiwać funkcjonalność ochrony przed skasowaniem lub odmapowaniem od hosta woluminu dyskowego, do którego były przesłane operacje wejścia/wyjścia w określonym przez użytkownika czasie.  i. Dostępne sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu dla podłączanych systemów operacyjnych (jeżeli jest wymagana licencja, należy dostarczyć licencje na całość oferowanych zasobów). |
| 2.3 | Obsługa wirtualnych dysków logicznych:  a. Minimalna ilość wspieranych wirtualnych dysków logicznych (LUN) dla całej (globalnej) puli dyskowej musi wynosić co najmniej 2000. Funkcjonalność LUN Masking i LUN Mapping.  b. Urządzenie musi umożliwiać stworzenie mirrorowanych LUN pomiędzy różnymi typami dysków, dla których awaria jednej kopii lustra musi być niezauważalna dla systemu hosta. |
| 2.4 | Funkcjonalność thin provisioning:  Urządzenie musi obsługiwać funkcjonalność thin provisioning dla wszystkich wolumenów. Musi istnieć możliwość wyłączenia tej funkcjonalności dla wybranych wolumenów. Należy dostarczyć licencję umożliwiającą korzystanie z funkcji thin provisioning na całą oferowaną pojemność urządzenia. |
| 2.5 | Kopie migawkowe:  Urządzenie musi mieć możliwość wykonywania natychmiastowej kopii danych (point-in-time copy). Funkcjonalność ta powinna być realizowana w trybie copy-on-write. Licencja powinna obejmować możliwość stworzenia co najmniej 60 kopii. |
| 2.6 | Migracja wolumenów logicznych:  Urządzenie musi mieć możliwość wykonania migracji wolumenów logicznych pomiędzy różnymi typami dysków wewnątrz macierzy bez zatrzymywania aplikacji korzystającej z tych wolumenów. Wymaga się, aby zasoby źródłowe podlegające migracji oraz zasoby do których są migrowane mogły być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (SAS, SSD, SATA). |
| 2.7 | Replikacja macierzy :  Urządzenie musi posiadać funkcjonalność replikacji danych przy użyciu synchronicznych oraz asynchronicznych transmisji danych przez łącza komunikacyjne IP oraz FC lub FCoE. Macierz musi przechowywać w pełni zsynchronizowaną kopię w odległości do 300km. Przy znacznie większej odległości, do 8000km, replikacje mogą działać asynchronicznie. Oba rodzaje replikacji muszą wspierać program Vmware Site Recovery Manager do odzyskiwania danych po awarii. Jeśli na obsługę powyższej funkcjonalności wymagana jest dodatkowa licencja, nie jest ona wymagana w tym postępowaniu. |
| 2.8 | Wirtualizacja zasobów:  Macierz musi mieć możliwość wirtualizacji zasobów znajdujących się na innych niż oferowane macierze dyskowe na potrzeby migracji danych. Migracja musi się odbyć w trybie bezprzerwowym. |
| 2.9 | Macierz musi mieć funkcjonalność wykonywania pełnej kopii lokalnych wolumenów logicznych z wykorzystaniem jedynie kontrolerów macierzy. Licencja powinna obejmować możliwość stworzenia co najmniej 60 kopii. |
| 2.10 | Macierz musi mieć możliwość dodawania kolejnych półek dyskowych oraz dysków bez przerywania pracy macierzy, dla dowolnej konfiguracji macierzy |
| 2.11 | Macierz musi posiadać funkcjonalność optymalizacji wykorzystania dysków SSD/Flash poprzez automatyczną identyfikację najbardziej obciążonych fragmentów wolumenów w zarządzanych zasobach dyskowych oraz ich automatyczną migrację na dyski SSD/Flash. Macierz musi również automatycznie rozpoznawać obciążenie fragmentów wolumenów na dyskach SSD/Flash i automatycznie migrować z dysków SSD/Flash nieobciążone fragmenty wolumenów. Macierz musi posiadać możliwość wykorzystania mechanizmu optymalizacji umiejscowienia danych pomiędzy przynajmniej 3 rodzajami dysków – SSD/Flash, Enterprise (SAS 10k) oraz NL-SAS/SATA, jak również przy wykorzystaniu dwóch dowolnych z wyżej wymienionych typów. Opisany powyżej proces optymalizacji musi posiadać funkcję włączenia/wyłączenia na poziomie pojedynczego wolumenu. Jeśli na obsługę powyższej funkcjonalności wymagana jest dodatkowa licencja, nie jest ona wymagana w tym postępowaniu. |
| 2.12 | Macierz musi mieć możliwość aktualizacji oprogramowania macierzy (firmware) w trybie online. |
| 2.13 | Macierz musi umożliwiać tworzenie wolumenów o pojemności nie mniejszej niż 250 TB |
| 2.14 | Do macierzy należy dołączyć przewody zasilające oraz 8 przewodów światłowodowych o długości 5m. |
| **3** | **Inne** |
| 3.1 | Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu. |
| 3.2 | Oferowane produkty (urządzenia, sprzęty) w przedmiotowym postępowaniu o udzielenie zamówienia publicznego muszą spełniać wymagania norm CE, tj. muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE. |
| 3.3 | Wszystkie oferowane urządzenia muszą być fabrycznie nowe. |
| 3.4 | Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. |
| 3.5 | Urządzenie musi współpracować z siecią energetyczną o parametrach w przedziale 200V- 230V, 50 Hz. |
| 3.6 | Macierz dyskowa musi być objęta gwarancją świadczoną w reżimie 9x5 (5 dni w tygodniu, okno zgłoszeń 9h) przez okres 60 miesięcy z reakcją na następny dzień roboczy od momentu zgłoszenia usterki. Ze względu na 60 miesięczny okres Zamawiający wymaga, aby usługi serwisowe świadczone były wyłącznie przez producenta oferowanego sprzętu, nie dopuszcza się świadczenia serwisu przez autoryzowanych partnerów producenta. |
| 3.7 | Zgłoszenia usterek muszą być akceptowane przez producenta zarówno drogą email jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.). Linia telefoniczna musi być czynna 24 godziny na dobę, 7 dni w tygodniu również w dni świąteczne. |
| 3.8 | Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia przez cały okres obowiązywania gwarancji. |

1. **Przełączniki sieciowe spełniające następujące wymagania (2 szt.):**

Para przełączników (po 1 szt. na każdą z dwóch lokalizacji) z min. 24 portami SFP+. Przełączniki powinny mieć skonfigurowane:

* Zarządzanie po SSH oraz GUI
* Odpowiednie VLAN do komunikacji podłączanych urządzeń
* NTP, DNS, SNMP
* Protokół zapobiegający powstawaniu pętlom
* Harmonogram, który aktywuje skrypt wyłączający oraz włączający porty o danej godzinie

Do przełączników powinno być dostarczone 20 szt. kompatybilnych wkładek SFP+ 10G.

**Usługi switche:**

* Wykonawca będzie zobowiązany wykonać bazową konfigurację przełączników (hasło, mgmt, ntp, elrp, vlan, dns, snmp).
* Konfiguracja skryptu oraz harmonogramu, która zostanie wykonana wg. omówionego i zaakceptowanego przez zamawiającego scenariusza (należy zaplanować odpowiednie okna backupowe, w ten sposób aby backup został skutecznie wykonany w trakcie okna czasowego).
* Dokonfigurowanie posiadanej przez Zamawiającego infrastruktury Fortinet (Fortigate i Fortiswitche) (dodatkowe polityki, etc)
* Instalacja i uruchomienie, testowanie.
* Dokumentacja powykonawcza.

**SPECYFIKACJA SWITCHY:**

1. Przełącznik musi być wyposażony w 8 portów uplink SFP+ 1/10G. Jeśli do pracy w trybie 10G wymagana jest licencja, to musi być ona dostarczona.
2. Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet
3. Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów.
4. Wszystkie porty przełącznika muszą mieć możliwość wsparcia szyfracji MACsec 128/256-bit. Jeśli funkcjonalność wymaga dodatkowej licencji, to nie musi być ona dostarczona
5. Wysokość urządzenia 1U montowana w standardowym 19” Rack
6. Przełącznik musi posiadać wbudowany zasilacz 230V
7. Przełącznik musi posiadać możliwość łączenia z innymi przełącznikami w stos z wydajnością min. 40 Gb/s.
8. Przełącznik musi umożliwiać stworzenie stosu złożonego z 8 przełączników.
9. Stos musi zachowywać się jak jedno urządzenie logiczne, a w szczególności mieć możliwość bezpośredniej konfiguracji wszystkich fizycznych portów dostępnych na przełącznikach połączonych w stos, oraz posiadać jeden adres IP w celu zarządzania stosem.
10. Porty przełącznika, używane do łączenia przełączników w stos, muszą mieć możliwość pracy jako standardowe porty transmisji danych SFP+ z przepustowością 10 Gb/s
11. Nieblokująca architektura o wydajności przełączania min. 256 Gb/s
12. Szybkość przełączania min. 190 Milionów pakietów na sekundę
13. Temperatura pracy przełącznika w zakresie min. 0o do 50o C
14. Tablica MAC adresów min. 32 tys.
15. Pamięć operacyjna: min. 1 GB pamięci DRAM
16. Pamięć flash: min. 1 GB pamięci Flash
17. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
18. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
19. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
20. Obsługa Q-in-Q IEEE 802.1ad
21. Obsługa Quality of Service
22. Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p
23. Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ
24. 8 kolejek priorytetów na każdym porcie wyjściowym
25. Obsługa kolejek Strict Priority
26. Obsługa kolejek Weighted Round Robin
27. Obsługa WRED (Weighted Random Early Detection)
28. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
29. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
30. Obsługa CDPv2
31. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
32. Możliwość instalacji min. dwóch wersji oprogramowania – firmware
33. Możliwość przechowywania min. 10 wersji konfiguracji w plikach tekstowych w pamięci Flash
34. Możliwość monitorowania zajętości CPU oraz pamięci
35. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
36. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
37. Dedykowany port konsoli szeregowej RJ45
38. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika

**Obsługa Routingu IPv4**

1. Sprzętowa obsługa routingu IPv4 - forwarding
2. Pojemność sprzętowej tabeli routingu min. 8 000 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego IPv4
5. RIP v1/v2
6. OSPFv2 - możliwość rozszerzenia przez licencje
7. BGPv4 - możliwość rozszerzenia przez licencje
8. IS-IS - możliwość rozszerzenia przez licencje
9. Policy Based Routing dla IPv4
10. Obsługa DHCP/BootP Relay dla IPv4 z możliwością wysłania zapytań jednocześnie do min. 4 serwerów

**Obsługa Routingu IPv6**

1. Sprzętowa obsługa routingu IPv6 - forwarding
2. Pojemność tabeli routingu min. 4 000 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego dla IPv6
5. RIPng
6. OSPF v3 – możliwość rozszerzenia przez licencje
7. BGPv4 – możliwość rozszerzenia przez licencje
8. IS-IS – możliwość rozszerzenia przez licencje
9. Obsługa 6to4 (RFC 3056)
10. Obsługa MLDv1 (Multicast Listener Discovery version 1)
11. Obsługa MLDv2 (Multicast Listener Discovery version 2)
12. Policy Based Routing dla IPv6
13. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

**Obsługa Multicastów**

1. Statyczne przyłączanie do grupy multicast
2. Filtrowanie IGMP
3. Obsługa PIM-SM
4. Obsługa PIM-DM – możliwość rozszerzenia przez licencje
5. Obsługa PIM-SSM – możliwość rozszerzenia przez licencje
6. Obsługa Multicast VLAN Registration - MVR
7. Obsługa IGMP v1 - RFC 1112
8. Obsługa IGMP v2 - RFC 2236
9. Obsługa IGMP v3 - RFC 3376
10. Obsługa IGMP v1/v2/v3 snooping
11. Możliwość konfiguracji statycznych tras dla Routingu Multicastów

**Bezpieczeństwo**

1. Obsługa logowania do sieci Network Login
   1. IEEE 802.1x based Network Login
   2. MAC based Network Login
   3. Web-based Network Login
2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
3. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation
4. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x, MAC authentication - RFC 3580
5. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink lub portach dołączonych do przełączników obsługujących IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging
6. Automatyczne włączenie DHCP snooping oraz ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication – poprzez RADIUS VSA
7. Przełącznik musi posiadać mechanizm pozwalający na wyłączenie uwierzytelniania na porcie za pomocą RADIUS VSA np. w przypadku wykrycia bezprzewodowego punktu dostępowego, który „przejmuje” rolę uwierzytelniania klientów
8. Obsługa Guest VLAN dla IEEE 802.1x
9. Możliwość przekierowania na Captive Portal podczas logowania do sieci
10. Obsługa wymuszenia autoryzacji w celu zmiany autoryzacji (VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176
11. Obsługa TACACS+ (RFC 1492)
12. Obsługa RADIUS Authentication (RFC 2865)
13. Obsługa RADIUS Accounting (RFC 2866)
14. RADIUS per-command Authentication
15. Obsługa RADIUS over TLS (RadSec) – RFC 6614
16. Bezpieczeństwo MAC adresów
17. ograniczenie liczby MAC adresów na porcie
18. zatrzaśnięcie MAC adresu na porcie
19. możliwość wpisania statycznych MAC adresów na port/vlan
20. Możliwość wyłączenia MAC learning
21. Zabezpieczenie przełącznika przed atakami DoS
22. Networks Ingress Filtering RFC 2267
23. SYN Attack Protection
24. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
25. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
26. Adres MAC źródłowy i docelowy plus maska
27. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
28. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
29. Numery portów źródłowych i docelowych TCP, UDP
30. Zakresy portów źródłowych i docelowych TCP, UDP
31. Identyfikator sieci VLAN - VLAN ID
32. Quality of Service IEEE 802.1p oraz DiffServ
33. Flagi TCP
34. Obsługa fragmentów
35. Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
36. Możliwość konfiguracji min. 8 000 reguł na wejściu i 1000 reguł na wyjściu
37. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI
38. Obsługa bezpiecznego transferu plików SCP/SFTP
39. Obsługa DHCP Option 82
40. Obsługa IP Security – Trusted DHCP Server
41. Obsługa IP Security – DHCP Snooping and Guard
42. Obsługa IP Security - Gratuitous ARP Protection
43. Obsługa IP Security – DHCP Secured ARP/ARP Validation
44. Obsługa IP Security – IP Source guard
45. Ograniczanie przepustowości (rate limiting) na portach wyjściowych oraz ruchu wybranego poprzez ACL
46. Obsługa wykrywania periodycznego zaniku linku (Port-Flap). Musi istnieć możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu oraz reakcji polegającej na wyłączeniu portu na stałe lub na wskazany czas. Zdarzenie musi być raportowane poprzez Trap SNMP i/lub Syslog.

**Bezpieczeństwo sieciowe**

1. Przełącznik musi umożliwiać funkcję umożliwiającą statyczne skonfigurowanie portu głównego i zapasowego. W stanie normalnym, czyli bez awarii, jest używany port główny, a port zapasowy jest nieaktywny. Gdy port wskazany jako główny ulegnie awarii, czyli wykryje brak połączenia (link down), to port zapasowy się automatycznie aktywuje.
2. Obsługa redundancji routingu VRRP
3. Obsługa STP (Spanning Tree Protocol) IEEE 802.1D
4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
6. Obsługa PVST+
7. Obsługa ERPS / G.8032
8. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów
9. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników
10. Obsługa LACP w ramach MLAG

**Zarządzanie**

1. Obsługa synchronizacji czasu SNTP lub NTP
2. Zarządzanie przez SNMP v1/v2/v3
3. Zarządzanie przez przeglądarkę WWW – protokół http i https
4. Możliwość zarządzania przez XML API
5. Telnet Serwer/Klient dla IPv4 / IPv6
6. SSH2 Serwer/Klient dla IPv4 / IPv6
7. Ping dla IPv4 / IPv6
8. Traceroute dla IPv4 / IPv6
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów
10. Sprzętowa obsługa sFlow
11. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
12. Obsługa RMON2 (RFC 2021)
13. Obsługa autentykacji poprzez certyfikaty X509v3 dla protokołów SSH, Syslog oraz RADIUS

**Inne**

1. Współpraca z oprogramowaniem zarządzającym oferowanym przez producenta przełączników.
2. Współpraca z systemem zarządzającym w chmurze oferowanym przez producenta przełączników.
3. Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników.
4. Wbudowany DHCP Serwer i klient z możliwością definicji opcji (np. opcje 43, 60, 78 itp.)
5. Wsparcie standardu IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging
6. Obsługa skryptów CLI
7. Obsługa funkcji TCL/Tk w skryptach CLI
8. Obsługa skryptów Python 3.x
9. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
10. Możliwość uruchamiania skryptów
    1. Ręcznie
    2. O określonym czasie lub co wskazany okres czasu
    3. Na podstawie wpisów w logu systemowym

**GWARANCJA SWITCHE:**

Warunki gwarancyjne:

Za wyjątkiem wkładek SFP+ Wykonawca zapewni dożywotnią ograniczoną (do 5 lat od daty zakończenia produkcji) gwarancję realizowaną bezpośrednio przez producenta lub autoryzowany serwis.

W ramach umowy gwarancyjnej Wykonawca zapewni dostęp do najnowszych aktualizacji oprogramowania firmowego (ang. firmware).

Na wkładki SFP+ Wykonawca zapewni minimum 12 miesięczną gwarancję obowiązującą przez cały okres jego posiadania realizowaną bezpośrednio przez producenta lub autoryzowany serwis.

Warunki serwisu:

Sprzęt będzie w okresie gwarancji objęty serwisem świadczonym przez autoryzowany kanał serwisowy producenta. Serwis obejmuje bezpłatną podmianę sprzętu, wsparcie techniczne realizowane przynajmniej w dni robocze oraz możliwość pobierania aktualizacji oprogramowania.

Podmiana sprzętu następuje po uprzedniej weryfikacji i akceptacji konieczności wymiany sprzętu przez inżyniera wsparcia technicznego.

Jeżeli zgłoszenie takie zostanie zaakceptowane do godz. 13:00 dnia roboczego, sprzęt na podmianę zostanie wysłany następnego dnia roboczego z magazynu producenta.

Zgłoszenia będą przyjmowane w dni robocze drogą pisemną lub telefoniczną na wskazany nr telefonu, email lub stronę internetową.

Minimalny czas reakcji pomocy technicznej: 1 dzień roboczy.

Wymogi dotyczące autoryzacji usług gwarancji i serwisu (na etapie dostawy):

W przypadku gdy wymienione w specyfikacji usługi gwarancji i serwisu dla przedmiotowych urządzeń sieciowych nie są realizowane bezpośrednio przez producenta lub wymagają wykupienia od producenta kontraktów serwisowych:

w ramach dostawy wykonawca musi dostarczyć potwierdzenie wykupienia od producenta urządzeń wymaganych do świadczenia wyżej wymienionych usług kontraktów serwisowych lub w przypadku gdy takowe kontrakty nie są oferowane przez producenta potwierdzenie/świadectwo autoryzacji przez producenta w zakresie usług gwarancji i serwisu dla firmy serwisowej która będzie świadczyć wymienione w specyfikacji usługi gwarancji i serwisu dla przedmiotowych urządzeń sieciowych.

**UWAGI:**

Wykonawca jest zobowiązany na swoją odpowiedzialność zaplanować realizację i dostarczyć wszystkie dodatkowe elementy takie jak min. patchcordy, wkładki GBIC, okablowanie i materiały montażowe, które będą niezbędne do wykonania zadania w taki sposób, aby zapewniała prawidłowe działanie infrastruktur dostarczonej infrastruktury. Jeżeli zajdzie taka konieczność, wykonawca musi dostarczyć takie materiały, także do posiadanej przez zamawiającego infrastruktury w celu połączenia jej z dostarczanymi w ramach obecnego postępowania elementami. W razie potrzeby zamawiający zapewni możliwość przeprowadzenia wizji lokalnej na miejscu w dni robocze w godzinach 7:00 – 15:00.

1. **Komputer zarządzający macierzą backup-ową** (1 szt.)

Zarządzanie macierzą, na której będą przechowywane backupu, musi być realizowane bez dostępu do sieci LAN. Wykonawca musi dostarczyć dedykowane stanowisko zarządzania macierzą, które będzie się cechować poniższymi parametrami:

|  |  |  |
| --- | --- | --- |
|  | Typ | Komputer stacjonarny. |
|  | Wydajność obliczeniowa | Procesor min. 4-rdzeniowy, wielowątkowy, klasy x86-64, taktowanie bazowe min. 3.2 GHz, procesor powinien osiągać w teście <http://www.cpubenchmark.net>   wynik min.  13800 pkt. |
|  | Pamięć operacyjna RAM | min. 8 GB,  - wymagane zachowanie 1 slotu wolnego na późniejszą rozbudowę |
|  | Parametry pamięci masowej | * 500GB (M.2 NVMe SSD) * Wolny slot 2,5-calowy dla dysku SSD |
|  | Wydajność grafiki | Zintegrowana grafika (jednoczesna obsługa trzech wyświetlaczy, rozdz. 1920x1080pxl, obsługa 4K, pow. 2GB wykorzystywanej pamięci, DX12, OpenGL 4.5)  Min. 1x HDMI, 1x DP, 1x VGA (złącze analogowe wymagane obligatoryjnie bez żadnych przejściówek) |
|  | Wyposażenie multimedialne | 24-bitowa karta dźwiękowa, zintegrowana z płytą główną, zgodna z High Definition, porty słuchawek i mikrofonu na przednim panelu obudowy. |
|  | Obudowa | Komputer powinien być wyposażony w dobrze wentylowaną i funkcjonalną obudowę, aby zapewnić odpowiednią cyrkulację powietrza oraz zabezpieczenie przed przegrzaniem.  Zasilacz o mocy max 150W, umożliwiający bezproblemową prace komputera w zaoferowanej konfiguracji.  Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie oraz wpisanym w BIOS. |
|  | Bezpieczeństwo | (TPM) Zintegrowany z płytą główną układ służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. |
|  | System operacyjny – w formularzu oferty należy wpisać pełną nazwę oferowanego oprogramowania | Zainstalowany system operacyjny 64-bit, który posiada wbudowane mechanizmy, bez użycia dodatkowych aplikacji (bez jakichkolwiek emulatorów, implementacji lub programów towarzyszących), zapewniające:   1. Polską wersję językową, 2. Możliwość instalacji i poprawnego działania oprogramowania dostępnego w ramach posiadanych przez Zamawiającego licencji Microsoft Office 2016; 3. Możliwość instalacji i poprawnego działania aplikacji wykorzystywanych przez Zamawiającego, oraz poprawnej obsługi powszechnie używanych urządzeń peryferyjnych (drukarek, skanerów, kser), 4. Dostępność aktualizacji i poprawek do systemu u producenta systemu bezpłatnie i bez dodatkowych opłat licencyjnych z możliwością wyboru instalowanych poprawek. 5. Możliwość zdalnej, automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, 6. Możliwość automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechniania systemu operacyjnego inicjowanego i wykonywanego w całości przez sieć komputerową, 7. Możliwość wdrożenia nowego obrazu przez zdalną instalację, 8. Graficzne środowisko instalacji i konfiguracji, 9. Możliwość udostępniania i przejmowania pulpitu zdalnego, 10. Możliwość udostępniania plików i drukarek, 11. Możliwość blokowania lub dopuszczenia dowolnych urządzeń peryferyjnych za pomocą polityk sprzętowych (np. przy użyciu numerów identyfikacyjnych sprzętu), 12. Zapewnienie wsparcia dla większości powszechnie używanych urządzeń (drukarek, urządzeń sieciowych, standardów USB, urządzeń Plug & Play, WiFi, 13. Wyposażenie systemu w graficzny interfejs użytkownika w języku polskim, 14. Zapewnienie pełnej kompatybilności z oferowanym sprzętem, 15. Zintegrowanie z systemem modułu pomocy dla użytkownika w języku polskim, 16. Zintegrowanie z systemem modułu wyszukiwania informacji, 17. Możliwość wykonania kopii bezpieczeństwa (całego dysku, wybranych folderów, kopii przyrostowych) wraz z możliwością automatycznego odzyskania wersji wcześniejszej, 18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników, 19. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacja dostępna u producenta nieodpłatnie bez ograniczeń czasowych, 20. Licencja na system operacyjny musi być nieograniczona w czasie, pozwalać na wielokrotne instalowanie systemu na oferowanym sprzęcie bez konieczności kontaktowania się przez Zamawiającego z producentem systemu lub sprzętu, 21. Oprogramowanie powinno posiadać certyfikat autentyczności lub unikalny kod aktywacyjny, 22. dostęp do wsparcia technicznego systemu operacyjnego na okres nie mniejszy od planowanego czasu eksploatacji komputera.   Zamawiający nie dopuszcza w systemie możliwości instalacji dodatkowych narzędzi emulujących działanie systemów. |
|  | Certyfikaty i standardy | Deklaracja zgodności CE  Certyfikaty dla producenta komputera: ISO 9001; ISO 14001, ISO 27001 oraz ISO 50001 |
|  | Warunki gwarancji | 3-letnia gwarancja, czas reakcji serwisu w ramach gwarancji do końca następnego dnia roboczego.  Serwis gwarancyjny urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |
|  | Wymagania dodatkowe | 1. Wbudowane porty w płytę główną: 2. 1 x DisplayPort 3. 1 x HDMI 4. 1x VGA 5. 6 portów USB Typ A w tym min. 4 porty USB 3.0   Wymagana ilość i rozmieszczenie portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, kart PCIe itp.   1. 1 port USB 3.0 Typ C 2. Port słuchawek 3. Komputer wyposażony w Bluetooth w wersji 5.0 4. Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługęWoL, PXE 2.0, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem z poziomu konsoli zarządzania - łącznie z obsługą stanu S3 (uśpienie) oraz S4-S5 (hibernacja i wyłączenie). 5. Płyta główna wyposażona w:  * 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, * min. 1 złącze SATA 3.0,  1. Dołączony nośnik ze sterownikami lub sterowniki do pobrania ze strony producenta |

1. **KVM** (1 szt.)

* Montaż w szafie rack 19” z możliwością wysuwania.
* Wysokość 1U
* Monitor 17 Cali (chowany w obudowie 1U)
* Wymagany port VGA
* Pełnowymiarowa klawiatura
* Touchpad
* Porty SPHD – 1szt.
* Port USB – 1szt.
* Porty PS/2 – 1szt. (lub dodatkowy port USB).

1. **Serwer - wymagania techniczne**  (1 szt.)

**Obudowa**

* Typu RACK, wysokość 2U;
* Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
* Możliwość zainstalowania 1 dysków twardych hot plug 3,5”;
* Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych;
* Zainstalowane 2 szt. dysków SSD M.2 SATA 240GB w RAID-1 podpięte do sprzętowego kontrolera;
* Zainstalowane 3 szt. SSD 3,84TB, RAID-5 podpięte do sprzętowego kontrolera
* Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.
* Możliwość zainstalowania dedykowanego wewnętrznego napędu LTO.

**Płyta główna**

* Dwuprocesorowa;
* Wyprodukowana i zaprojektowana przez producenta serwera;
* Możliwość instalacji procesorów 40-rdzeniowych;
* Zainstalowany moduł TPM 2.0;
* 7 złącz PCI Express generacji 4 w tym:
  + 4 fizyczne złącza o prędkości x16;
  + 3 fizyczne złącza o prędkości x8;
  + Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
  + Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e;
* 32 gniazda pamięci RAM;
* Obsługa minimum 4 TB pamięci RAM DDR4;
* Obsługa 10 TB pamięci operacyjnej w konfiguracji RAM DDR4 + pamięć nieulotna;
* Wsparcie dla technologii:
  + Memory Scrubbing;
  + SDDC;
  + ECC;
  + Memory Mirroring;
  + ADDDC;
* Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci);
* Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express)  nie zajmujące klatek dla dysków hot-plug.

**Procesory**

* Jeden procesor nie więcej niż 8-rdzeniowy, architektura x86\_64;

**Pamięć RAM**

* 256 GB pamięci RAM;
* DDR4 Registered 3200Mhz.

**Kontrolery LAN**

Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:

* 4x 1Gbit Base-T;
* Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

Interfejsy LAN zainstalowane w slotach PCI-e:

1. **W celu optymalizacji i przyspieszenia procesów backup-owych oraz wydzielenia sieci kopii zapasowych z sieci produkcyjnej, wykonawca zobowiązany jest dostarczyć czteroportową kartę 10Gb do posiadanego przez zamawiającego serwera Fujitsu RX2540 M6.**
2. **Montaż i konfiguracja serwera.**
3. **Instalacja oprogramowania VMware ESXi.**
4. **Migracja obecnego środowiska backupu Veeam na nowy serwer backupu.**
5. **Podłączenie i rekonfiguracja istniejącej biblioteki taśmowej, dla potrzeb serwera backupu.**
6. **Konfiguracja VLANów na przełącznikach dla potrzeb systemu.**
7. **Konfiguracja routingu oraz firewalla dla potrzeb systemu.**
8. **Zakup wraz z instalacją oraz konfiguracją na serwerze fizycznym systemu operacyjnego Windows Server Standard x64 - w najnowszej wersji (licencje na wszystkie Core procesorów proponowanej konfiguracji).**
9. **Wdrożenie funkcji bezpieczeństwa (antywirus, IPS, Web/DNS filtering) na nowo zainstalowanym sprzęcie.**
10. **Oprogramowanie backup-owe**Oprogramowanie musi być kompatybilne z obecnym. Aktualnie posiadamy: Veeam Backup Essentials Universal Perpetual License. Includes Enterprise Plus Edition features. Licencja musi obejmować minimum 10 maszyn wirtualnych i być licencją z 3 letnim kontraktem serwisowym.

Parametry równoważności:

•Oprogramowanie musi współpracować z infrastrukturą VMware w wersji, 6.0, 6.5, 6.7, 7.0 oraz Microsoft Hyper-V 2012, 2012 R2, 2016 oraz 2019. 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 Całkowite koszty posiadania

•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 musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli.

•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.

•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 aktualizacji pola „notatki” na wirtualnej maszynie

•Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backup-owym lub przed i po wykonaniu zadania snapshota. •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)

•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 oferować zarządzanie kluczami w przypadku utraty podstawowego klucza •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 wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej

•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

•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 backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn

•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 (GrandfatherFather-Son)

•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.

•Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.

•Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 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)

•Oprogramowanie musi umożliwiać 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 taką 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, Microsoft Azure Stack oraz Amazon EC2

•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 - ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs o Mac - HFS, HFS+ o Windows - NTFS, FAT, FAT32, ReFS •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 dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.

•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 włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat

•Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.

•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.

•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 Ograniczenie ryzyka

•Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.

•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

• Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere

• 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.

• Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

1. **Konfiguracja backupu oraz testowe odtworzenie jednej maszyny**
2. **Montaż zakupionego sprzętu w szafach rack**
3. **Wykonanie dokumentacji po wdrożeniowej**
4. **Sprzęt dostarczony do realizacji zamówienia musi być fabrycznie nowy (rok produkcji 2023) i pochodzić z oficjalnego kanału dystrybucji producenta.**
5. **Wykonawca zapewnia dostarczenie kompletnego systemu wraz z niezbędnymi elementami typu: zasilacze, karty pamięci, wkładki SFP, okablowanie sygnałowe i zasilające wraz z oprogramowaniem i licencjami niezbędnymi do zrealizowania wymaganej funkcjonalności.**
6. **Dostarczone oprogramowanie musi pochodzić z oficjalnego kanału dystrybucji producenta.**
7. **Wykonanie i dostarczenie Zamawiającemu dokumentacji powykonawczej. Dokumentacja powykonawcza musi być dostarczona w formie elektronicznej, na elektronicznym nośniku danych, w poniższych formatach danych:**
8. **doc/x – edytowalny (zgodny z Microsoft Word);**
9. **pdf – nieedytowalny, pełna dokumentacja (zgody z Adobe Reader).**
10. **Prace wdrożeniowe i integracyjne należy przeprowadzać nie zakłócając bieżącej pracy szpitala**
11. **Konfiguracje istniejących elementów sieci można również wykonywać popołudniami lub w weekendy**
12. **Szkolenie dla 2 administratorów odbywające się w siedzibie Zamawiającego w ilości co najmniej 15 godzin. Nie wykorzystane godziny szkoleniowe będą przeznaczone na wsparcie zdalne i telefoniczne.**

**Wdrożenie**

1. Przedmiot zamówienia z części A musi zostać zainstalowany, skonfigurowany, wdrożony i uruchomiony przez Wykonawcę zgodnie z wymaganiami Zamawiającego i przy jego współudziale.
2. Na wdrożenie i uruchomienie powinny składać się następujące etapy:

* opracowanie, w porozumieniu z Zamawiającym projektu technicznego obejmującego szczegóły implementacyjne rozwiązania:
* instalację systemu w najnowszej i rekomendowanej wersji;
* instalację, konfigurację i uruchomienie systemu w środowisku Zamawiającego zgodnie z zaakceptowanym przez niego projektem;
* prace wdrożeniowe dotyczące w szczególności konfiguracji i dostosowania działania systemu, które wynikną z aktualnych potrzeb Zamawiającego;
* opracowanie dokumentacji powykonawczej obejmującej:
  + opis rozwiązania;
  + schematy i topologie połączeń;
  + konfigurację oprogramowania wraz ze szczegółowym omówieniem zaimplementowanych funkcjonalności;
  + zalecenia powdrożeniowe obejmujące:
    - procedury dla administratorów;
    - procedury backupów;
    - procedury awaryjne.

**Część B – Audyt weryfikujący podniesienie poziomu bezpieczeństwa**

Po zakończeniu wdrożenia części A zamówienia Wykonawca wykona audyt.

Celem audytu jest wykazanie przez Wykonawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu zamówienia w części A, zgodnie z zarządzeniem 8/2023/BBIiCD PREZESA NARODOWEGO FUNDUSZU ZDROWIA w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u Zamawiającego formie ankiety wysłanej do NFZ. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa

Audyt musi być przeprowadzony przez:

1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;

2) co najmniej dwóch audytorów posiadających:

a) certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub

b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub

c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

1. Certified Internal Auditor (CIA);
2. Certified Information System Auditor (CISA);
3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność,akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
5. Certified Information Security Manager (CISM);
6. Certified in Risk and Information Systems Control (CRISC);
7. Certified in the Governance of Enterprise IT (CGEIT);
8. Certified Information Systems Security Professional (CISSP);
9. Systems Security Certified Practitioner (SSCP);
10. Certified Reliability Professional;
11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.