Załącznik 2 do SWZ DZP.382.1.14.2024 – Opis przedmiotu zamówienia

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L.P. | **NAZWA SPRZĘTU**  Minimalne parametry wymagane przez Zamawiającego | **Liczba sztuk** | **OPIS TECHNICZNY OFEROWANEGO SPRZĘTU**  Należy wskazać wszystkie elementy składowe oferowanego sprzętu w odniesieniu do kolumny z lewej strony | **INDEX** |
| 1. | **MACIERZ DYSKOWA (DEDYKOWANE URZĄDZENIE STORAGE DO PRZECHOWYWANIA DANYCH I TWORZENIA KOPII ZAPASOWYCH)**  Wymagane minimalne parametry techniczne:  1. Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów.  2.Deduplikator musi być wyposażony w minimum 2 kontrolery pracujące w trybie active-passive lub active-active. Deduplikator nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. W przypadku awarii kontrolera wszystkie procesy musi przejąć drugi kontroler.  3. Przestrzeń użytkowa po zbudowaniu RAID 6 musi wynosić min 56TB. Pula ta ma być chroniona 1 dyskiem hot-spare lub osobną przestrzenią przeznaczoną na użytek hot spare równą pojemności 1 dysku. Rozmiar RAW pojedynczego dysku nie może być większy niż 14 TB. Dodatkowo wymagane jest zastosowanie co najmniej 4 dysków SSD SAS o pojemności RAW min 1.92 TB jako cache pod zapis backupu. Wymagana pojemność użytkowa rozumiana jest jako pojemność dostępna po konfiguracji RAID i odliczeniu rezerwy na dyski/przestrzeń spare i dostępna dla hostów bez uwzględnienia jakichkolwiek mechanizmów kompresji, czy deduplikacji.  4.Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej, tolerującej jednoczesną awarię 2 dysków bez utraty danych. Urządzenie musi umożliwiać bezpieczne usuwanie danych zgodnie ze standardem DoD 5220.22-M poprzez mechanizm nadpisywania danych.  5. Co najmniej 256GB pamięci cache na cały deduplikator (dwa kontrolery). Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania.  6. Urządzenie musi posiadać minimum:  4 porty Ethernet 10 Gb/s z możliwością obsługi każdym portem Ethernet protokołów CIFS, NFS, wszystkie porty wyposażone we wkładki optyczne.  7. Wymagane wsparcie dla FC, iSCSI, NFS, CIFS.  8. Zarządzanie deduplikatorem (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu deduplikatora w tym monitorowanie wydajności obiektów takich jak:  - cały deduplikator  - kontrolery  - CPU  - porty front-end  - porty logiczne  - dyski  - file systemy  Pod kątem parametrów takich jak:  - operacje wejścia/wyjścia IOPS  - przepustowość (KB/s lub MB/s)  - czas odpowiedzi (latency)  - średnie użycie (w % dla CPU)  Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI urządzenia do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych.  Wymagany dostęp do informacji o wykorzystanej przestrzeni.  Wymagana możliwość tworzenia wielu użytkowników deduplikatora w oparciu o wbudowane role. Rozwiązanie musi umożliwiać tworzenie własnych ról.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje to należy wymienić je w opisie przedmiotu zamówienia oraz należy je uwzględnić w cenie ofertowej.    9. Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Dane muszą być poddane także procesowi kompresji.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje to należy wymienić je w opisie przedmiotu zamówienia oraz należy je uwzględnić w cenie ofertowej.  Wymagana także obsługa deduplikacji na źródle, co pozwala ograniczyć zużycie sieci.  10. Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni, z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni.  Wymagana możliwość skonfigurowania polityki filtrowania zapisywanych plików poprzez wykluczenie ich konkretnych rozszerzeń.  Wymagana możliwość ograniczenia dostępu do udostępnionych udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp.  11. Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file systemów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów, które będą zabezpieczone przed modyfikacją oraz usunięciem przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Musi być możliwość odtworzenia danych z dowolnej kopii (snapshot) wykonanej w ramach harmonogramu. Odtworzenie danych z jednej kopii nie może uniemożliwiać odtworzenia danych z innej kopii z innego punktu w czasie. Dostarczenie tej funkcjonalności jest wymagane na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora.  Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM).  12. Urządzenie musi umożliwiać replikację danych do drugiego urządzenia w ramach tej samej rodziny oferowanego deduplikatora. Replikacja musi się odbywać w trybie asynchronicznym. Wymagana możliwość ograniczenia ilości przesyłanych danych poprzez ich deduplikację oraz kompresję.  Deduplikator musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60 min) lub konkretnych okien czasowych (np. w każdą sobotę o godz. 20:00).  Wymagana możliwość zastosowania funkcjonalności typu AirGap czyli fizyczne wyłączanie portów dedykowanych do replikacji w czasie kiedy replikacja nie jest wykonywana. Dopuszcza się realizację tej funkcjonalności poprzez zastosowanie dodatkowego oprogramowania.  13. Urządzenie musi wspierać co najmniej następujące aplikacje do backupu: Commvault, Veritas NetBackup, Veeam Backup&Replication.  14. Wymagane szyfrowanie danych zapisywanych na deduplikatorze algorytmem AES256 lub silniejszym.  15. Deduplikator musi posiadać możliwość upgrade’u firmware-u kontrolerów bez przerywania dostępu do danych.  Urządzenie przystosowane do napraw w miejscu instalacji oraz wymiany elementów bez konieczności jego wyłączania.  Urządzenie musi umożliwiać zdalne zarządzanie.  Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej 2024 i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego.  Deduplikator musi zostać objęty minimum 3 letnim okresem gwarancji producenta | 1 szt |  | 169907 |
| **2.** | **Przełącznik sieciowy, min 12 portów optycznych 1/10/25 Gbps + uplink 10G/1G 10GBaseT RJ-45 z akcesoriami**   1. Urządzenie musi posiadać min. 12 portów optycznych 1/10/25 Gbps definiowanych modułem optycznym 2. Urządzenie musi posiadać slot na moduł rozszerzeń. Zamawiający wymaga obsługi następujących modułów: 3. 2x 100G/40G QSFP+ Network Module 4. 8x 25G/10G/1G Network Module 5. 8x 10G/1G 10GBaseT RJ-45 Multigigabit Network Module 6. W momencie dostawy, każde z urządzeń musi być wyposażone w moduł wymienny obsadzony 8 portami miedzianymi RJ45 Multigigabit 1G/10 Gbps 7. Musi być możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:    1. Przepustowość w ramach stosu – 1Tb/s    2. Min. 8 urządzeń w stosie    3. Zarządzanie poprzez jeden adres IP    4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad    5. Możliwość współdzielenia mocy zasilaczy (grupy do 4 urządzeń w stosie) tzn. zasilacze stanowią zasób wspólny dla grupy przełączników (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania” mocy dla innych jednostek w stosie, w tym dla przełączników wymagających większej mocy dla PoE, jeśli takie są zainstalowane w stosie)    6. Jeżeli do funkcjonalności stakowania potrzebne są dodatkowe moduły, muszą być dostarczone z urządzeniem wraz z kablem o długości min. 50cm. 8. Urządzenie musi posiadać redundantne i wymienne moduły wentylatorów 9. Urządzenie musi posiadać wymienny zasilacz 230V o mocy min. 700W i oraz możliwość wymiany na zasilacz prądu stałego DC lub na zasilacz większy o mocy min. 1100W i instalacji w trybie hot plug identycznego zasilacza redundantnego 10. Urządzenie musi umożliwiać podtrzymanie zasilania z portów PoE podczas restartu urządzenia 11. Urządzenie musi wspierać IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności) 12. Bufor pakietów – min. 16MB 13. Pamięć DRAM urządzenia– min. 16GB 14. Pamięć flash – min. 16GB 15. Zdolność przełączania min. 1000 Gbps samodzielnego przełącznika i do 2000 Gbps w stosie 16. Obsługa minimum:     1. 4.000 sieci VLAN     2. 32.000 adresów MAC     3. 39.000 tras IPv4     4. 19.000 tras IPv6     5. 8000 tras multicastowych     6. 4000 wpisów QoS 17. Obsługa protokołu NTP 18. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping 19. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:     1. IEEE 802.1w Rapid Spanning Tree     2. Per-VLAN Rapid Spanning Tree (PVRST+)     3. IEEE 802.1s Multi-Instance Spanning Tree     4. Obsługa 128 instancji protokołu STP 20. Obsługa protokołu LLDP i LLDP-MED. 21. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC 22. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego 23. Obsługa funkcji serwera DHCP 24. Mechanizmy związane z bezpieczeństwem sieci:     1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)     2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN     3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL     4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X     5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC     6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X     7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem     8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176     9. 8000 wpisów dla list kontroli dostępu (Security ACE)     10. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www)     11. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard     12. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard)     13. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+     14. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)     15. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128)     16. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing)     17. Funkcja Private VLAN 25. Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia. 26. Mechanizmy związane z zapewnieniem jakości usług w sieci:     1. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi     2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek     3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)     4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP     5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting)     6. Kontrola sztormów dla ruchu broadcast/multicast/unicast     7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP 27. Obsługa protokołów routingu:     1. dla IPv4: RIP, OSPF (min. 900 ścieżek), EIGRP Stub     2. Funkcjonalności Policy-based routing     3. Obsługa protokołu redundancji bramy (VRRP) 28. Urządzenie musi obsługiwać tworzenie sprzętowo statystyk ruchu w oparciu o NetFlow, wielkość tablicy monitorowanych strumieni wynosi min. 64 000. 29. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN 30. Przełącznik musi posiadać definiowane wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.) 31. Urządzenie musi posiadać port konsoli 32. Urządzenie musi posiadać dedykowany port Ethernet do zarządzania out-of-band 33. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją 34. Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku 35. Urządzenie musi obsługiwać protokoły SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 36. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów 37. Przełącznik musi posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych 38. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą 39. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. 40. Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU. 41. Przełącznik objęty serwisem producenta lub partnera przy wsparciu producenta z reakcją następnego dnia roboczego  **Akcesoria:**   * Przełącznik wyposażony w moduł do łączenia w stos urządzeń  i zasilania wraz z kablem stakującym * 6 szt, – wkładki SFP+ RJ-45 30m * 4 szt, – wkładki SFP+ SingleMode 10GB * 4 szt, – wkładki QSFP 10/25GB Single Mode   Przewody zasilające umożliwiają podpięcie do UPS | 2 szt. |  | 169908 |
|  | **Gwarancje, licencje oraz inne wymagania**  * Dostarczony sprzęt powinien być objęte gwarancją producenta świadczoną przez autoryzowany serwis. * Dostarczony sprzęt objęty jest gwarancją i wsparciem technicznym na okres 3 lat. * obsługi zgłoszeń serwisowych na zasadzie NBD (trybie 8x5) - zgłoszenia przyjmowane są przez telefon, e-mail – obsługa, w języku polskim lub angielskim, * Usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) w ciągu 2 dni roboczych od momentu zgłoszenia usterki; * naprawa w miejscu instalacji sprzętu * w przypadku awarii dyski twarde pozostają własnością Zamawiającego, * serwis urządzeń realizowany będzie zgodnie z wymaganiami normy ISO 9001 lub równoważnej. * Wykonawca gwarantuje, że każdy produkt który zostanie dostarczony do Uniwersytetu Śląskiego:   Jest nowy (rok produkcji nie wcześniej niż 2024), pochodzić bezpośrednio od producenta lub od autoryzowanego dystrybutora, zakupiony na terenie Europejskiego Obszaru Gospodarczego. |  |  |  |
|  | **Wdrożenie:**  * Instalacja dostarczonego sprzętu w siedzibie Zamawiającego. * Instalacji i aktualizacji dostarczonego wraz ze sprzętem oprogramowania (firmware, inne   niezbędne do jego prawidłowej konfiguracji) oraz wszystkich urządzeń będących elementami wdrożenia. W tym również oprogramowania jeżeli będzie taka potrzeba.   * Konfiguracji urządzenia zgodnie z potrzebami Zamawiającego * Wykonaniu dokumentacji powdrożeniowej (w formie pisemnej edytowalnej) zawierającej opis skonfigurowanego deduplikatora. * Przeszkoleniu przez Wykonawcę w siedzibie Zamawiającego 2 administratorów w zakresie konfiguracji i eksploatacji dostarczonego sprzętu. |  |  |  |