**OPIS PRZEDMIOTU ZAMÓWIENIA**

**PAKIET I**

**WYMAGANE PARAMETRY TECHNICZNE**

**Po zmianie z dnia 22.04.2022 r.**

**I. Urządzenie typu firewall – 2 szt.**

1. Musi być dostarczone jako samodzielne, dedykowane fizyczne urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej rozwiązania musi występować moduł zarządzania i moduł przetwarzania danych.

2. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.

3. Urządzenie musi być wyposażone w dedykowany port zarządzania out-of-band.

4. Brak ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.

5. Urządzenie musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.

6. Obsługa dla IPv6.

7. Funkcjonalność statycznej i dynamicznej translacji adresów NAT między IPv4 i IPv6.

8. Reguły zabezpieczeń firewall muszą być tworzone zgodnie z ustaloną polityką opartą o profile oraz obiekty.

9. Polityka zabezpieczeń firewall musi uwzględniać przynajmniej takie parametry jak: adresy IP źródłowe i docelowe, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie.

10. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich dostępnych portach.

11. Interfejs administracyjny urządzenia musi być w języku polskim.

12. Firewall musi działać w następujących trybach:

a. routera (tzn. w warstwie 3 modelu OSI),

b. przełącznika (w warstwie 2 modelu OSI),

c. transparentnym

d. pasywnego nasłuchu.

Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych biorących udział w transmisji.

13. Zarządzanie firewallem musi odbywać się z linii poleceń (CLI) oraz z graficznej konsoli GUI. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Dopuszcza się, aby polityki mogły być tworzone tylko z graficznej konsoli GUI.

14. Musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP, mapowanie 1 adres publiczny na 1 adres prywatny oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.

15. Musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenia muszą umożliwiać stworzenie co najmniej 6 klas dla różnego rodzaju ruchu sieciowego.

16. Firewall musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.

17. Obsługa protokołu Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.

18. Obsługa protokołów routingu dynamicznego, nie mniej niż RIP, OSPF oraz BGP.

19. Firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

20. Musi posiadać osobny zestaw polityk definiujący ruch zaszyfrowany SSL oraz SSH, który należy poddać lub wykluczyć z operacji deszyfrowania rozdzielny od polityk bezpieczeństwa.

21. Musi posiadać funkcjonalność automatycznego pobierania listy stron WWW lub adresów IP z zewnętrznego systemu oraz używania ich w politykach bezpieczeństwa.

22. Ochrona przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony informującej użytkownika o próbie pobrania pliku i możliwości kontynuowania lub zaniechania pobrania.

23. Urządzenie musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.

24. Firewall musi identyfikować co najmniej 2500 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS m.in.: Skype, Tor, BitTorrent, eMule.

25. Możliwość definiowania własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta.

26. System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie wyłącznie na podstawie rozszerzenia.

27. Urządzenie musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Urządzenie musi umożliwiać konfigurację tuneli VPN w trybie route-based VPN.

28. Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN oraz IPSec.

29. Firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną).

30. Producent urządzenia musi udostępniać dedykowanego klienta binarnego VPN dla platform Windows, Mac oraz Android.

31. Urządzenie musi transparentnie ustalać tożsamość użytkowników sieci w oparciu o Active Directory oraz Ms Exchange. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym Citrix oraz Windows Terminal Services, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.

32. Musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach.

33. Urządzenie musi obsługiwać nie mniej niż 3 wirtualne routery posiadające odrębne tabele routingu.

34. Rozwiązanie musi umożliwiać rozbudowę o możliwość wykrywania domen DGA i ruchu tunelowanego przez DNS. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 36 miesięcy.

35. Musi mieć możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesje w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.

36. Musi mieć możliwość wyboru sposobu blokowania ruchu w politykach bezpieczeństwa.

37. Musi istnieć możliwość ustawienia cichego blokowania ruchu bez wysyłania RST, blokowanie z wysłaniem RST tylko do klienta, blokowanie z wysłaniem RST tylko do serwera, blokowanie z wysłaniem RST do klienta i serwera jednocześnie.

38. Urządzenie musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.

39. Musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i kategorii stron WWW.

40. Urządzenie musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.

41. Urządzenie musi być dostarczone w konfiguracji z minimum 8 portami Ethernet 1Gb/s

42. Urządzenie musi posiadać przepustowość w ruchu nie mniej niż 4 Gbps dla kontroli firewall z włączoną funkcją kontroli aplikacji. Przepustowość dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (ochrona IPS, antywirus, antyspyware, identyfikacja aplikacji) nie może być mniejsza niż 2 Gbps.

43. Urządzenie musi obsłużyć minimum 350 000 jednoczesnych sesji oraz 65 000 nowych połączeń na sekundę.

44. Urządzenie musi zapewniać wydajność przynajmniej 2.5 Gbps dla ruchu IPSec VPN i umożliwiać zestawienie przynajmniej 2500 równoczesnych tuneli site-to-site.

45. Urządzenie musi mieć wysokość maksymalnie 1U.

46. Urządzenie musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników pracujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi umożliwiać deszyfracje niezaufanego ruchu HTTPS i poddania go dalszej inspekcji.

47. Musi umożliwiać wykluczenie z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie co najmniej: kategoryzacji stron URL oraz dodania własnych wyjątków.

48. Musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (IPS, AV, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.

49. Urządzenie musi zapewniać zestawienie przynajmniej 1200 sesji SSL VPN.

50. Urządzenie musi posiadać funkcjonalność weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci lub wybranych jej zasobów. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia w ramach niniejszego postępowania.

51. Urządzenie musi posiadać funkcjonalność sterowania zachowaniem binarnego klienta VPN z poziomu systemu - połączenie automatyczne bądź ręczne przez użytkownika a także umożliwiać sprawdzenie czy klient posiada zainstalowane oprogramowanie antywirusowe. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia w ramach niniejszego postępowania.

52. Urządzenie musi posiadać funkcjonalność zestawienia tuneli VPN SSL bez konieczności instalowania klienta na stacji końcowej – clientless VPN. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania.

53. Urządzenie musi posiadać funkcjonalność zestawienia tuneli VPN SSL za pomocą instalowania klienta na stacji końcowej – clientless VPN. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający wymaga jej dostarczenia w ramach tego postępowania na okres minimum 36 miesięcy.

54. Musi posiadać możliwość uruchomienia funkcji wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS). W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 36 miesięcy.

55. Urządzenie musi posiadać możliwość uruchomienia funkcji inspekcji antywirusowej, kontrolującej przynajmniej protokoły: SMTP, HTTP, POP3, IMAP oraz podstawowe rodzaje plików. Baza AV musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 36 miesięcy.

56. Urządzenie musi umożliwiać filtrowanie stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza przypisania URL do kategorii musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 36 miesięcy.

57. Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.

58. Firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 36 miesięcy.

59. Urządzenie musi zapewniać moduł przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików (przynajmniej exe, dll, pdf, jar, apk, pliki MS Office, ELF, BAT, JS, VBS, PS1, shell script, HTA, linki w wiadomościach e-mail) przechodzących przez firewall w celu ochrony przed zagrożeniami typu zero-day. Informacja zwrotna na temat wykrytego złośliwego oprogramowania musi zostać dostarczona na firewall w czasie nie dłuższym jak 5 minut. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików.

60. Musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive i Active-Active w przypadku pracy z drugim takim samym urządzeniem posiadającym taki sam zestaw licencji.

61. Musi pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej.

62. Urządzenie nie może znajdować się na liście „koniec sprzedaży” oraz „koniec wsparcia” producenta.

63. Serwis dostępu do najnowszej wersji oprogramowania, serwis sprzętowy i ewentualne licencje/subskrypcje na aktualizacje bazy aplikacji muszą być ważne przynajmniej przez okres 36 miesięcy.

64. Pomoc techniczna oraz szkolenia z produktu muszą być świadczone w miejscu dostawy. Usługi te muszą być świadczone w języku polskim.

65. Świadczenie gwarancyjnych usług serwisowych odbywać się będzie zgodnie z opisem w załączniku C do SWZ Wymagania dotyczące dostawy instalacji, konfiguracji oraz uruchomienia Pakiet I.

66. Jeżeli funkcjonalność wymaga wykupienia dodatkowej licencji wtedy Zamawiający wymaga jej dostarczenia na okres 36 miesięcy.

**II. Macierz dyskowa – 2 szt.**

Ogólne

1. System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” i zajmować maks. 2U w tej szafie.

2. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia).

3. Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii.

4. Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy lub musi być dostarczona licencja na dwukrotność dostarczanej pojemności.

5. Dostarczana macierz musi umożliwiać takie podłączenie półek aby awaria lub/i usunięcie jednej z półek nie powodowało utraty dostępu do danych znajdujących się na pozostałych modułach.

6. Oferowana macierz musi obsługiwać min. 260 dysków wykonanych w technologii hot-plug. Wszystkie zainstalowane dyski hot-plug, z wyłączeniem dysków SSD stosowanych jako rozszerzenie pamięci Cache kontrolerów, muszą być dostępne dla zapisu danych Użytkownika.

7. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów (tzw. „półek dyskowych”) w rozmiarze 2U pozwalająca umieścić do min. 24 dysków 2,5” typu hotplug dla dysków SAS i SSD oraz w rozmiarze 2U dla min. 12 dysków 3,5” typu hotplug NL-SAS i SSD oraz półki gęstego upakowania dla min. 50 dysków typu hotplug NL-SAS;

8. Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych (tj. 2,5” + 3,5” + gęstego upakowania).

Pojemność macierzy:

9. Macierz musi zostać dostarczona z dyskami zapewniającymi pojemność surową min. 65TB. Pojemność jednego dysku nie może być większa niż 4 TB.

Kontrolery

10. Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami;

11. Każdy z kontrolerów macierzy musi posiadać po minimum 32 GB pamięci podręcznej Cache (możliwość rozbudowy do 64GB) – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu;

12. Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 800GB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD,

13. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk.

14. Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia;

15. Kontrolery macierzy obsługują funkcjonalność kompresji danych.

16. Kontrolery macierzy obsługują funkcjonalność deduplikacji w trybie in-line.

17. Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach.

18. Każdy z kontrolerów RAID powinien posiadać dedykowany minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.

19. Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej z minimum 4 rdzeniami,

20. Kontrolery macierzy muszą obsługiwać do 130 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów

21. Oferowana macierz musi mieć wyprowadzone 4 porty FC 16Gb/s (obsadzone modułami LC MMF) do dołączenia serwerów bezpośrednio lub do sieci san na każdy kontroler RAID.

a. Macierz musi umożliwiać wymianę połowy portów do transmisji danych na porty 2x 10Gb/s Base-T iSCSI.

b. Macierz musi umożliwiać wymianę połowy portów do transmisji danych na porty 2x 10Gb/s SFP+ iSCSI.

c. Macierz musi umożliwiać wymianę połowy portów do transmisji danych na porty 2x SAS 12Gb/s.

d. Macierz musi umożliwiać wymianę połowy portów do transmisji danych na porty 2x FC 32Gb/s.

e. Macierz musi umożliwiać wymianę połowy portów do transmisji danych na porty 4x FC 16Gb/s.

f. Macierz musi umożliwiać wymianę połowy portów do transmisji danych na porty 2x 10Gb/s SFP+ CIFS/NFS.

22. Wymiana portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych

23. Macierz musi posiadać możliwość obsługi operacji plikowych I/O w sieci NAS w obrębie zainstalowanych kontrolerów. Protokoły dostępu: CIFS, NFS. W przypadku obsługi protokołów CIFS i NFS wymagana jest funkcjonalność agregacji przepustowości dla interfejsów dedykowanych do obsługi tych protokołów. Obsługa protokołów CIFS i NFS musi odbywać się jednocześnie . Jeśli funkcjonalność ta wymaga dodatkowej licencji, to nie ma konieczności jej dostarczania w niniejszym postępowaniu. (opcja rozbudowy)

Poziomy RAID

24. Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:

a. Raid-1

b. Raid-10

c. Raid-5

d. Raid-6

e. Raid-50

f. Raid-0.

Dyski

25. Oferowana macierz musi wspierać dyski hot-plug:

a. dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s

b. dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm,

26. Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania;

27. Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex

28. Macierz musi obsługiwać min. 260 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami;

29. Możliwość rozbudowy oferowanego modelu macierzy do minimum 520 dysków bez migracji i przenoszenia danych - jedynie poprzez wymianę modułu kontrolerów macierzy (bez konieczności wymiany posiadanych dysków, półek dyskowych, bez konieczności przenoszenia danych/ istniejącej struktury grup dyskowych/LUN, jak również z zachowaniem istniejącej gwarancji producenta na półki dyskowe i dyski;

30. Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) lub wirtualna przestrzeń zapasowa:

a. Macierz posiada możliwość konfiguracji dysku hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID lub zapasowa przestrzeń wirtualna wielkości 33% zabezpieczanej pojemności.

b. Macierz posiada możliwość konfiguracji dysku hot-spare dedykowanego dla zabezpieczenia tylko wybranej grupy dyskowej RAID lub zapasowa przestrzeń wirtualna wielkości 33% zabezpieczanej pojemności.

31. W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess) lub nie wymaga zwolnienia zapasowej przestrzeni wirtualnej.

32. Macierz musi pozwalać na zaszyfrowanie danych zapisanych na wszystkich obsługiwanych dyskach SSD-SAS, HDD-SAS oraz HDD NL-SAS minimum kluczem AES256-bit – jeżeli w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą.

33. Macierz musi umożliwiać zaszyfrowanie całej dostępnej powierzchni użytkowej minimum kluczem AES256-bit.

Opcje programowe

34. Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 2048 kopii migawkowych

35. Macierz musi umożliwiać zdefiniowanie min. 6000 woluminów (LUN)

36. Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 1024 ścieżek logicznych FC

37. Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów

38. Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową

39. Macierz musi posiadać wsparcie dla systemów operacyjnych : Microsoft Windows Server 2012R2, 2016, 2019, SuSE Linux Enterprise Server, Red Hat Linux Enterprise Server, HP-UNIX, IBM AIX, SUN Solaris, Vmware Vsphere;

40. Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.

41. **Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych; Jeśli funkcjonalność ta wymaga dodatkowej licencji, to jest konieczne jej dostarczanie w niniejszym postępowaniu.**

42. Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror Jeśli funkcjonalność ta wymaga dodatkowej licencji, to nie ma konieczności jej dostarczania w niniejszym postępowaniu. (opcja rozbudowy)

43. Macierz musi obsługiwać mechanizm ochrony priorytetów obsługi wybranych zasobów – za taki mechanizm uznaje się funkcję typu ‘cache partitioning’ lub ‘storage partitioning’.

44. Macierz musi obsługiwać adresację IP v.4 i IP v.6

45. Wraz z macierzą należy dostarczyć oprogramowanie lub moduły programowe typu plug-in pozwalające na integracje macierzy w środowiskach Vmware w zakresie obsługi mechanizmów: Vmware VAAI, Vmware VVOL, Vmware MultiPath IO – z subskrypcją do bezpłatnej aktualizacji w całym okresie obowiązywania gwarancji

46. Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy.

47. Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SSAS, NLSAS. Macierz musi pozwalać na definiowanie różnych polityk i zasad migrowania danych w obrębie tej samej macierzy. Mechanizm AST musi być obsługiwać funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) mierzonej jako maksymalny czas opóźnień operacji I/O wykonywanych przez serwer/środowisko/aplikację. Mechanizm AST musi pozwalać na definiowanie okna czasowego dla zbierania pomiarów wydajności operacji I/O oraz okna czasowego dla migrowania danych wg ustalonych zasad i polityk – minimalny definiowany czas trwania w/w operacji (długość okna czasowego) nie może być dłuższy niż 8 godzin. Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O. Jeśli funkcjonalność ta wymaga dodatkowej licencji, to nie ma konieczności jej dostarczania w niniejszym postępowaniu. (opcja rozbudowy)

48. Macierz musi wspierać usługi VSS (Volume ShadowCopy Services) w systemach klasy Microsoft Windows Sever – wymagane jest dostarczenie niezbędnego oprogramowania / sterowników VSS pozwalających na obsługę VSS przy maksymalnej pojemności i liczbie dysków obsługiwanych przez oferowaną. W czasie trwania gwarancji wymaga się bezpłatnego dostępu do nowych wersji oprogramowania i sterowników

49. Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy tej klasy, z zachowaniem obsługi operacji I/O dla serwerów podłączonych do migrowanej macierzy tj. do migrowanych zasobów LUN

50. Macierz wspiera rozwiązania klasy ‘klastra macierzowego’ tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami protokołami FC oraz iSCSI. Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC oraz iSCSI, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy. Pod użytym pojęciem ‘wysoka dostępność zasobów dyskowych’ należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzą, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Funkcjonalność ‘klastra macierzowego’ musi pozwalać na automatyczne i ręczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. Automated/manual failover).

Jeśli funkcjonalność ta wymaga dodatkowej licencji, to nie ma konieczności jej dostarczania w niniejszym postępowaniu. (opcja rozbudowy)

51. Macierz w dostarczonej konfiguracji musi obsługiwać deduplikację i kompresję danych na dyskach wbudowanych w macierzy (nie dopuszcza się główek, kompresji zewnętrznej, programowej itp.) w następujących trybach równocześnie oraz niezależnie na poziomie każdego LUN:

o Sama deduplikacja wybranego LUN;

o Sama kompresja wybranego LUN;

o Kombinacja technologii kompresji i deduplikacji wybranego LUN;

o Brak użycia technologii kompresji i deduplikacji dla wybranego LUN;

Zarządzanie

52. Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej

53. Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.

54. Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora

55. Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI

Gwarancja i serwis

57. Uszkodzone dyski twarde pozostają u Zamawiającego.

58. Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia.

59. Po zakończeniu okresu gwarancji musi być zapewniony przez producenta lub autoryzowanego partnera serwisowego producenta rozwiązanie bezpłatnego dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy oraz do kolejnych wersji oprogramowania zarządzającego w okresie minimum 2 lat.

60. System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół. Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta – musi być do tego wykorzystany dedykowany system serwisowy macierzy.

61. Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych

62. Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia

63. Producent macierzy lub autoryzowany partnera producenta musi umożliwiać odpłatne wydłużenie gwarancji do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki.

64. Producent lub autoryzowany partnera producenta oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać adres internetowy strony producenta lub autoryzowanego partnera producenta macierzy, gdzie można zweryfikować wymagane informacje.

65. Świadczenie gwarancyjnych usług serwisowych odbywać się będzie zgodnie z opisem w załączniku C do SWZ Wymagania dotyczące dostawy instalacji, konfiguracji oraz uruchomienia Pakiet I.

66. Wykonawca wraz z uruchomieniem macierzy dyskowej zainstaluje i wdroży oprogramowanie do cyfrowego deponowanie i archiwizowania danych – repozytorium.

67. Repozytorium musi umożliwiać użytkownikom tworzenie bezpiecznych zasobów i długoterminowe ich archiwizowanie.

68.Pliki muszą być deponowane i archiwizowane w repozytorium bezpośrednio przez przeglądarkę internetową, bez instalacji dodatkowego oprogramowania na stacjach klienckich.

69. System musi zapewniać usługę gromadzenia, przetwarzania i archiwizowania różnych formatów plików.

70. System musi gromadzić informacje o poprzednich wersjach materiałów, identyfikować użytkowników oraz rejestrować z jakich zasobów dany użytkownik korzystał. Wszystkie wcześniejsze wersje materiałów muszą być dostępne.

71. DO zgromadzonych danych musi być dostęp za pomocą różnych zewnętrznych narzędzi.

72. Autoryzacja użytkownika powinna odbywać się za pomocą serwera usług katalogowych.