**Załącznik nr 1 do SWZ**

Zamówienie – kompleksowe i całościowe dostarczenie rozwiązania IT w celu polepszenia cyberbezpieczeństwa.

W ramach tego rozwiązania dostarczone zostanie rozwiązanie IT w postaci systemu zabezpieczeń danych, systemu redundancji danych w chmurze, zarządzalnego urządzenia sieciowego, serwerów fizycznych, macierzy dyskowej, serwerowych systemów operacyjnych i oprogramowania bezpieczeństwa oraz zasilania awaryjnego.

Przeprowadzone zostanie również w ramach zamówienia szkolenie specjalistyczne w zakresie dostarczanych i wdrażanych rozwiązań IT.

Celem zamówienia jest zwiększenie poziomu cyberbezpieczeństwa ww. podmiotów poprzez wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych.  Celem jest wdrożenia mechanizmów i środków zwiększających na ataki z cyberprzestrzeni.

W wyniku podjętych działań przyczyniających się do sprawnego i bezpiecznego działania systemów informatycznych, podniesie się poziom cyberbezpieczeństwa.

W celu wzmocnienia odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych konieczny jest zakup sprzętu, oprogramowania i usług informatycznych w obszarze cyberbezpieczeństwa jako kompleksowego i efektywnego rozwiązania.

Skutkiem realizacji będzie skuteczne zabezpieczenie systemów informatycznych przed cyberprzestępczością w kontekście: ochrony danych osobowych (RODO), potencjalnej utraty danych, ujawnienia wrażliwych danych osobom nieuprawnionym albo umożliwienia atakującym zniszczenia dokumentów lub danych, co zapewni ciągłość pracy oraz zwiększy poczucie bezpieczeństwa.

**Przedmiot obejmuje kompleksowe rozwiązanie:**

1. Rozwiązanie IT – system zabezpieczeń danych;
2. System redundancji w chmurze;
3. Zarządzalne urządzenia sieciowe:
4. 1 szt. przełącznika sieciowego
5. 3 Access Point;
6. Serwery fizyczne – 3 szt.
7. Macierz dyskowa – 1 szt.
8. Serwerowe systemy operacyjne i oprogramowanie bezpieczeństwa:
9. System operacyjny
10. Oprogramowanie do wirtualizacji

Zasilanie aw

1. aryjne
2. Szkolenia specjalistyczne

Wykonawca w ramach postępowania zobowiązany jest do wykonania co najmniej następujących usług związanych z montażem i konfiguracją dostarczanej infrastruktury sprzętowej:

1. Wykonanie Projektu Technicznego dostarczanej infrastruktury sprzętowej, który będzie składał się co najmniej z następujących elementów:

- dokładna specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów,

- nazwy oraz szczegółowa adresacja poszczególnych elementów,

- planowana konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsca, zaprojektowanie kompleksowego systemu ochrony danych opartego na funkcjach macierzy oraz oprogramowania standardowego z uwzględnieniem specyfiki całego projektu,

- wymagane działania ze strony Zamawiającego w celu poprawnego montażu i konfiguracji,

- harmonogram prac.

Projekt techniczny musi zostać wykonany po wcześniejszej analizie środowiska wykonanej przez Wykonawcę oraz musi zostać zaakceptowany przez Zamawiającego.

1. Instalacja oraz konfiguracji oprogramowania zgodnie z wytycznymi Zamawiającego (m.in. wirtualizacja, backup, domena AD)
2. Instalacja i konfiguracja systemu firewall (m.in. reguły dostępu, do Internetu oraz komunikacji wewnętrznej, Remote Access VPN, SSL VPN, integracja z AD)
3. Testy rozwiązania.
4. Instruktaż dla administratorów demonstrujący sposób zarządzania środowiskiem.
5. Dostarczenie dokumentacji powykonawczej infrastruktury sprzętowej i oprogramowania standardowego, która będzie składała się co najmniej z następujących elementów:

- specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów oraz numerami seryjnymi poszczególnych elementów,

- końcowe nazwy oraz szczegółowa adresacja poszczególnych elementów,

- konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsc

- komplety poświadczeń do całej infrastruktury – wymagana zmiana haseł domyślnych – dostarczone jako osobny załącznik w postaci zaszyfrowanego pliku kdbx,

- dokumentacja techniczna w formie elektronicznej do każdego elementu w języku polskim lub angielskim,

- szczegóły dotyczące instalacji i uruchomienia infrastruktury sprzętowej, w zakresie modernizacji infrastruktury Zamawiającego, zostaną ustalone pomiędzy Stronami w trakcie Analizy Przedwdrożeniowej,

- zamawiający zapewni odpowiedni zapas mocy oraz odpowiednie warunki środowiskowe w komorach serwerowni,

- po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników”.

Wymagania w zakresie instalacji i konfiguracji:

1. Montaż urządzeń w posiadanej szafie rack 42U w pomieszczeniu udostępnionym przez Zamawiającego.
2. Podłączenie urządzeń do listew zasilających PDU.
3. Aktualizacja oprogramowania układowego wszystkich komponentów.
4. Podłączenie do sieci LAN ( rekonfiguracja przełączników )

Wykonawca po zainstalowaniu i skonfigurowaniu sprzętu i oprogramowania będzie miał obowiązek przeprowadzenia instruktażu dla administratorów Zamawiającego w zakresie konfiguracji i zarządzania dostarczonego sprzętu oraz oprogramowania.

**UWAGA**

Wszystkie ewentualne nazwy własne i marki handlowe urządzeń i elementów zawarte w opisie przedmiotu zamówienia, zostały użyte w celu sprecyzowania oczekiwań jakościowych i technologicznych Zamawiającego.

Zamieszczone w specyfikacji nazwy technologicznych lub producentów kluczowych komponentów użyto jedynie w celu przykładowym.

Zamawiający informuje, że dopuszcza składanie ofert, w których poszczególne urządzenia bądź materiały wymienione w opisie przedmiotu zamówienia mogą być zastąpione urządzeniami bądź materiałami/elementami równoważnymi. Poprzez pojęcie materiałów/elementów i urządzeń równoważnych należy rozumieć materiały zapewniające uzyskanie parametrów technicznych nie gorszych od założonych w opisie przedmiotu zamówienia. Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia w stosunku do przewidzianych w niniejszym zaproszeniu, ani do zmiany ceny.

1. **Rozwiązanie IT – system zabezpieczeń danych**

**a) Next Generation Firewall**

**Wymagania Ogólne**

1. Muszą to być specjalizowane urządzenia sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako para wysokiej dostępności (HA) w trybach Active/Passive, Active/Active.

2. Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta. Producent oferowanego rozwiązania musi być obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls.

3. Urządzenia muszą umożliwiać działanie w następujących trybach pracy:

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

b. mostu (tzn. w warstwie 2 modelu OSI),

c. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; Musi pracować w trybie przezroczystego łączenia interfejsów w pary.).

d. w trybie pasywnego nasłuchu (sniffer/tap).

4. System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.

5. Urządzenia firewall muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu od zasobów służących do zarządzania urządzeniem.

6. Urządzenie musi posiadać dedykowane zasoby/rdzenie procesora/procesorów do funkcji zarządzania urządzeniem lub możliwość ustawienia dedykowanych zasobów/rdzeni procesora/procesorów do funkcji zarządzania urządzeniem.

7. Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.

8. Urządzenia firewall muszą wspierać protokół LACP.

9. Urządzenia firewall muszą zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).

10. Urządzenia firewall muszą działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.

11. Polityka zabezpieczeń firewall musi uwzględniać

a. adresy IP źródłowe i docelowe,

b. protokoły i usługi sieciowe,

c. aplikacje,

d. kategorie URL,

e. użytkowników aplikacji i grupy,

f. reakcje zabezpieczeń,

g. logowanie zdarzeń (początek i koniec sesji)

h. strefa wejściowa i wyjściowa

12. Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. 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 65535 dostępnych portach. Przy tym wydajność kontroli firewalla stanowego i kontroli aplikacji całego ruchu nie może być mniejsza, niż wskazano w wymaganiach wydajnościowych urządzeń.

13. Urządzenie musi wykrywać co najmniej 3700 predefiniowanych aplikacji wspieranych przez producenta (takich jak DNS over HTTPS, Telegram, Skype, Tor, BitTorrent, MQTT, Modbus, DNP3, Siemens S7) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.

14. Urządzenia firewall muszą pozwalać na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.

15. Urządzenia firewall muszą zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.

16. Urządzenia firewall muszą być wyposażone w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy dostarczyć odpowiednie dla minimum 30 administratorów.

17. Dostęp do urządzeń i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.

18. Urządzenia firewall muszą umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż:

a. baza lokalna,

b. serwer Radius,

c. serwer TACACS+,

d. serwer AD/LDAP.

Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH a dla dostępu GUI za pomocą certyfikatów kryptograficznych.

19. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:

a. Active Directory,

b. Terminal Services

20. Polityka kontroli dostępu (urządzeń firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości musi odbywać się również transparentnie.

21. Urządzenia firewall muszą pozwalać na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL.

22. Urządzenie musi dostarczać predefiniowane przez producenta raporty standardowe jak i możliwość tworzenia raportów niestandardowych. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu.

23. Urządzenie musi pozwalać na zapisanie raportów na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.

24. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:

a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia)

b. API

25. Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESX i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można potem wykorzystywać w polityce bezpieczeństwa urządzeń.

26. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.

27. Urządzenia firewall muszą obsługiwać 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 oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.

28. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

29. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami NAT.

30. Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju.

31. Urządzenia firewall muszą obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.

32. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa.

33. Wykonywanie operacji deszyfrowanie ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji. Musi zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.

34. Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL.

35. Dla deszyfrowania ruchu TLS 1.3 wymagane jest wsparcie dla X25519, X448 oraz minimum dla zestawów protokołów: TLS\_AES\_128\_GCM\_SHA256, TLS\_AES\_256\_GCM\_SHA384 oraz TLS\_CHACHA20\_POLY1305\_SHA256.

36. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.

37. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) i ustawiania dla aplikacji priorytetu oraz pasma.

38. Urządzenia firewall muszą umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. routing-based VPN).

39. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.

40. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.

41. Urządzenia firewall muszą zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tuneli SSH.

42. Wszystkie funkcjonalności muszą pochodzić od producenta. W przypadku gdy jakakolwiek funkcjonalność lub parametr ilościowy wymagają licencji, zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres 24 miesięcy od daty odbioru sprzętu.

43. Wykonawca zapewni wsparcie serwisowe (techniczne) i gwarancje dla systemu (zwana dalej wsparciem) będzie świadczone przez producenta lub autoryzowane przez producenta centrum serwisowe, niezależne od Wykonawcy, realizowane we współpracy z producentem, przez okres 24 miesięcy od daty odbioru sprzętu.

44. Dodatkowa funkcjonalność musi dostarczać ochronę antywirusową (ale nie równoważną z sandbox), anti-spyware i przed podatnościami systemów.Musi ona zapewniać co najmniej:

a. wykrywanie aktywności sieci typu Botnet na podstawie analizy behawioralnej,

b. sygnatury antywirusowe - wykrywanie wirusów i złośliwego oprogramowania znajdującego się w plikach wykonywalnych i typach plików,

c. sygnatury anti-spyware - wykrywanie aktywności typu command-and-control (C2), gdzie oprogramowanie szpiegowskie na zainfekowanym kliencie zbiera dane bez zgody użytkownika i/lub komunikuje się ze zdalnym napastnikiem,

d. sygnatury podatności - wykrywanie podatności systemowych, które napastnik mógłby próbować wykorzystać,

e. sygnatury command-and-control (C2) dla ruchu DNS,

f. informacje o adresach IP złośliwych hostów,

g. informacje o adresach IP podejrzanych hostów (wysokiego ryzyka).

45. Urządzenie musi wykrywać i blokować zagrożenia DNS w ruchu przechodzącym przez urządzenie bez potrzeby rekonfiguracji serwera DNS i bez potrzeby ustawiania firewall jako serwera DNS. Wykrywający i blokujący ruch do domen uznanych za złośliwe musi być sterowany (przekierowanie) za pomocą funkcji DNS Sinkholing.

46. Urządzenie musi posiadać i być dostarczone z funkcjonalnością systemu wykrywania i zapobiegania włamaniom (Intrusion Prevention System – IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System musi działać w warstwie 7 modelu OSI. Baza sygnatur systemu wykrywania i zapobiegania włamaniom musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł systemu wykrywania i zapobiegania włamaniom musi mieć możliwość wykluczania z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji lub zdefiniowanych serwisów, np. poprzez numer portu, protokół transportowy.

47. Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak co najmniej http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur AV musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent urządzenia na którym realizowana jest ta funkcja. Moduł AV musi mieć możliwość wykluczania z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji lub zdefiniowanych serwisów, np. poprzez numer portu, protokół transportowy.

48. Urządzenie musi zapewniać ochronę przed atakami typu spyware. Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub IPS lub antymalware lub dedykowany silnik antyspyware. Baza sygnatur antispyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik antispyware musi mieć możliwość wykluczenia z filtrowania specyficznego ruchu sieciowego na podstawie zarówno adresu źródłowego IP jak i adresu docelowego IP jak i rozpoznania aplikacji bez względu na numery portów, na których działa.

49. Urządzenie musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).

50. Urządzenia firewall muszą umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „SandBox” plików wykonywalnych PE i DLL przechodzących przez firewall. Systemy sandbox, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików, adresów IP, DNS i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik. Maksymalny interwał aktualizacji sygnatur 48 godzin.

51. System zabezpieczeń NGFW musi dodatkowo oferować możliwość identyfikacji w ruchu sieciowym i przesyłania do zintegrowanej usługi analizy dynamicznej (tzw. „sandbox”) plików następujących typów: wykonywalnych (PE), Microsoft Office, Adobe flash / PDF, archiwa: JAR, RAR, 7-ZIP, Android APK, Mac OSX, skrypty: BAT, JScript, PowerShell, VBS, Perl i Python. W przypadku potwierdzenia nieznanego ataku (tzw. “zero-day”), musi następować automatyczna aktualizacja systemu firewall nowymi sygnaturami opisującymi wykryte pliki malware lub ich zidentyfikowane złośliwe zachowania (np. wzorce komunikacji zwrotnej) w wyniku przeprowadzonej analizy.

52. Uruchomienie ochrony typu “sandbox” dla systemu zabezpieczeń NGFW musi być możliwe w następujących trybach:

a. Subskrypcji - bez dokupowania jakichkolwiek komponentów sprzętowych wyłącznie w oparciu o usługę chmurową producenta rozwiązania (uruchamianą na terenie EU)

b. Prywatnym - po zakupieniu dodatkowego urządzenia do analizy lokalnej

c. Hybrydowym - z wykorzystaniem zarówno subskrypcji i po zakupieniu urządzenia do analizy lokalnej.

53. W każdym z powyższych trybów, administrator systemu NGFW musi mieć możliwość konfiguracji rodzaju pliku, kontekstu użytej aplikacji, kierunku transmisji (wysyłanie / odbieranie) i miejsca analizy (chmura / urządzenie lokalne) dla celów definicji ruchu i klasyfikacji obiektów do analizy typu „sandbox”.

54. Rozwiązanie NGFW musi posiadać możliwość wysyłania plików do analizy w usłudze chmurowej “sandbox” producenta rozwiązania.

55. Urządzenia firewall muszą posiadać funkcję filtrowania URL.

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

57. Rozwiązanie musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania kategorii URL.

58. Urządzenia firewall muszą umożliwiać zabezpieczenie działania protokołu DNS poprzez procesowanie zapytań DNS w celu wykrywania i blokowania: zagrożeń, wycieku danych (exfiltracja).

59. System zabezpieczeń firewall musi być wyposażony w mechanizm automatycznego wyboru optymalnego trasowania WAN dla zdefiniowanej aplikacji, przy zapewnieniu jej maksymalnej wydajności, dostępności oraz bezpieczeństwa. Dla różnych technologii połączeń fizycznych WAN (np. LTE, DSL, MPLS, WiFi itd.) zakończonych w standardzie Ethernet, musi być możliwość ich ciągłego monitorowania w zakresie: straty pakietów, opóźnienia oraz odchylenia (tzw. jitter) jako parametrów decyzyjnych do dynamicznego wyboru najkorzystniejszej trasy. Zintegrowana funkcjonalność SD-WAN, musi działać bezpośrednio na urządzeniu, w oparciu o system centralnego zarządzania, bez konieczności dokupywania dodatkowych komponentów, poza subskrypcją.

60. System zabezpieczeń NGFW musi posiadać osobny zestaw polityk SD-WAN, definiujący najkorzystniejszy sposób dystrybucji kluczowego ruchu firmowego, rozdzielny od polityk bezpieczeństwa. Pojedyncza reguła SD-WAN musi uwzględniać następujące atrybuty ruchu: strefy bezpieczeństwa, adresy IP źródłowe i docelowe, aplikacje, porty usług, wartości klasyfikatorów jakościowych łącz (opóźnienie, strata pakietów, jitter) oraz metody korekcji błędów.

61. Urządzenia firewall muszą obsługiwać funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta musi być realizowana na bazie technologii SSL VPN oraz IPSec. Jeżeli oprogramowania klienta Remote Access VPN dla laptopów z systemem Windows wymaga licencji – należy dostarczyć licencję na maksymalną wydajność oraz maksymalną ilość dla oferowanego typu urządzeń.

62. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.

63. Urządzenie musi obsługiwać funkcjonalność zdalnych sesji VPN z wykorzystaniem każdej z poniższych metod:

a. z wykorzystaniem aplikacji klienckich zainstalowanych na stacjach roboczych (ang. desktop clients),

b. z wykorzystaniem aplikacji na platformy mobilne (ang. mobile clients),

c. z wykorzystaniem przeglądarki internetowej bez konieczności instalacji klienta (ang. clientless access).

64. Oprogramowanie klienta VPN musi posiadać możliwość weryfikacji kondycji bezpieczeństwa stacji zdalnej Windows i macOS co najmniej w zakresie sprawdzenia:

a. czy zainstalowano oprogramowanie antywirusowe i czy posiada ono aktualne sygnatury,

b. czy włączony jest osobisty firewall,

c. czy komputer jest komputerem w domenie Active Directory (dla Windows).

65. Oprogramowanie klienckie zdalnego dostępu musi posiadać bezpłatne wsparcie producenta w rozumieniu możliwości zakładania spraw serwisowych.

66. Rozwiązanie musi pozwalać na odseparowanie zdalnego komputera w przypadku stwierdzenia jego kompromitacji.

**UWAGA**: Wszystkie wymienione powyżej funkcje muszą być dostępne i realizowane przez firewall jednocześnie. Nie jest dopuszczalne, aby realizacja jakiejkolwiek funkcjonalności powodowała konieczność przełączenia urządzenia w inny tryb pracy ograniczający lub uniemożliwiający skorzystanie z innej wymaganej funkcji. Podobnie uruchomienie jakiekolwiek opisanej funkcji nie może spowodować wyłączenie lub ograniczenie działania innej funkcji wymaganej przez Zamawiającego.

Jednocześnie Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do złożenia wyjaśnień oraz prezentacji działania zaoferowanego urządzenia w przypadku powzięcia wątpliwości w tym zakresie.

**PARAMETRY SPRZĘTOWE**

Każde z urządzeń musi (poza wymaganiami wspólnymi), spełniać dodatkowo wymagania:

1. Urządzenie będzie pracowało w trybie HA (wymagane 2 sztuki).

2. Urządzenie musi być wyposażone w minimum:

a. 8 wbudowanych interfejsów 10/100/1000Mbps Ethernet (RJ45),

3. Urządzenie musi być wyposażone w zasób dyskowy, inny niż obrotowy HDD, o pojemności minimum 128GB na potrzeby systemu operacyjnego i logów.

4. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:

a. Minimum 2,5 Gbps dla rozpoznawania i kontroli aplikacji,

b. Minimum 1 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Anty-wirus, Anty-spyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia,

c. Minimum 34 000 nowych sesji na sekundę,

d. Minimum 190 000 równoległych sesji.

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

6. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 2000 reguł polityki bezpieczeństwa.

**Warunki serwisu technicznego i procedura zgłoszeń**

Wsparcie techniczne musi być świadczone w języku polskim.

Wsparcie techniczne musi być świadczone przez okres 24 miesięcy . W ramach świadczenia gwarancyjnego, w wypadku wystąpienia awarii zamawiający otrzyma część zamienną/urządzenie objęte gwarancją w trybie następnego dnia roboczego. Wraz z dostarczonym sprzętem będzie świadczony dostęp do strony pomocy technicznej producenta oraz możliwość pobierania aktualizacji oprogramowania związanego z oferowanym sprzętem.

**b) System do backupu maszyn wirtualnych i hostów fizycznych**

|  |  |
| --- | --- |
| **LP.** | **Wymagania funkcjonalno-techniczne (minimalne)** |
| 1 | Licencja na oprogramowanie musi pozwalać na pełne wykorzystanie sprzętowych zasobów serwera |
| 2 | Zarządzanie poprzez GUI |
| 3 | System działający w modelu serwer – klient |
| 4 | Możliwość szyfrowania kopii po stronie klienta w celu zapewnienia bezpieczeństwa donych przed dotarciem do serwera backupowego |
| 5 | System backupowy posiada funkcjonalność deduplikacji |
| 6 | Możliwość korzystania z różnych typów przestrzeni dyskowych do składowania kopii bezpieczeństwa |
| 7 | System posiada funkcjonalność tworzenia harmonogramu wykonywania kopii |
| 8 | Automatyczna weryfikacja kopii bezpieczeństwa |
| 9 | Tworzenie kopii bezpieczeństwa maszyn wirtualnych |
| 10 | Możliwość tworzenia kopii na LTO-5 i nowsze |
| 11 | Powiadomienia e-mail o wykonanych / niewykonanych kopiach bezpieczeństwa |
| 12 | Możliwość zaplanowania maksymalnej liczy przechowywanych kopii |

1. **System redundancji danych w chmurze**

|  |  |
| --- | --- |
| **Element konfiguracji** | **Wymagania minimalne** |
| Liczba procesorów | Min. 18 vCPU |
| Pamięć operacyjna | Min. 60GB RAM |
| Przestrzeń dyskowa | Min. 4.8TB SSD |
| Interfejsy sieciowe | Min. 1 szt. 1 Gbit/s |
| Transfer | Min. 30 TB z serwera Nielimitowany do serwer |
| Lokalizacja | W obszarze UE |

1. **Zarządzalne urządzenie sieciowe**

Zamawiający oczekuje dostawy 1 przełącznika sieciowego, spełniającego poniższe, minimalne wymagania:

|  |  |
| --- | --- |
| Parametr | Charakterystyka (wymagania minimalne) |
| Typ urządzenia | Przełącznik sieciowy |
| Porty | Przełącznik musi posiadać: 24 x 10/100/1000BaseT 4 x 1G/10G/25G/50G1 SFP 1 x RJ45 do zarządzania |
| Obudowa | 1U, umożliwiająca montaż w szafie rack 19 cali |
| Zdolność przełączania | Min. 440 Gbps |
| Przekazywanie (pakiet 64-bajtowy) | Min. 330 Mpps |
| Bezpieczeństwo | SSH |
| Rozmiar tablicy MAC | 32K |
| Bufor pamięci | 8MB |
| Procesor | Switch musi posiadać czterordzeniowy procesor o taktowaniu min. 1800MHz ARM, |
| Pamięć Ram | Switch musi posiadać pamięć RAM min. 8 GB |
| Pamięć Flash | Switch musi posiadać pamięć Flash min. 32 GB |
| Standardy | IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3ad IEEE 802.3z |
| Inne | Przełączniki sieciowe muszą mieć możliwość połączenia w jedną spójną logiczną całość (stos). Do przełącznika należy dostarczyć 4 szt. wkładek 10G MMF SR |
| Gwarancja | Min. 5 lat gwarancji producenta |

Zamawiający oczekuje dostawy 3 szt. Access Point, spełniającego poniższe, minimalne wymagania:

|  |  |
| --- | --- |
| Parametr | Charakterystyka (wymagania minimalne) |
| Typ urządzenia | Access point |
| Częstotliwość | 2,4 GHz  5 GHz |
| Maksymalna szybkość przesyłania danych | 1770 Mbit/s |
| Maksymalna szybkość przesyłania danych (2.4 GHz) | 570 Mbit/s |
| Maksymalna szybkość przesyłania danych (5 GHz) | 1200 Mbit/s |
| Prędkość transferu danych przez Ethernet LAN | 10,100,1000 Mbit/s |
| Standardy komunikacyjne | IEEE 802.11a, IEEE 802.11ac, IEEE 802.11ax, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.3af, IEEE 802.3at, IEEE 802.3az |
| Automatyczne MDI/MDI-X | Tak |
| MIMO | Tak |
| Typ MIMO | Multi User MIMO |
| Metoda rozszerzenia obrazu | DSSS, OFDM, OFDMA |
| Modulacja | 16-QAM, 64-QAM, 256-QAM, 1024-QAM, BPSK, CCK, QPSK |
| Szyfrowanie / bezpieczeństwo | WPA3, WPA, WPA2 Do przełącznika należy dostarczyć 4 szt. wkładek 10G MMF SR |
| Porty i interfejsy | Ethernet LAN (RJ-45) 1szt; USB 2.0 (USB typa A) 1szt. |
| Obsługa PoE | Tak |
| Maksymalne zużycie mocy | 16,5 W |
| Zakres wilgotności względnej | 5 - 93% |
| Zakres temperatur (eksploatacja) | 0 - 50 °C |
| Zakres temperatur (przechowywanie) | -40 - 70 °C |
| Dopuszczalna wilgotność względna | 5 - 93% |

1. **Serwer fizyczny – 3 szt.**

Zamawiający poniżej wyspecyfikował minimalne parametry dla jednego serwera, przy czym wymaga dostarczenia 3 sztuk serwerów, o spełniających co najmniej poniższe parametry:

|  |  |
| --- | --- |
| **Element konfiguracji** | **Wymagania minimalne** |
| Obudowa | Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do mocowania kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia)  Serwer wyposażony w zdejmowany panel przedni z zamkiem chroniącym przed nieuprawionym dostępem do dysków oraz możliwością dołożenia czujnika otwarcia obudowy współpracującego z BIOS/UEFI. |
| Procesor | Dwa procesory dwunastordzeniowe, pracujące z częstotliwością bazową min. 2.0GHz i osiągające w testach SPECrate2017\_int\_base wynik nie gorszy niż 216 punktów, dla testu oferowanego modelu serwera z 2 procesorami.  Płyta główna wspierająca zastosowanie procesorów od 8 do 60 rdzeni, mocy do min. 350W i taktowaniu CPU do min. 3.7GHz. |
| Liczba procesorów | Min. 2 procesory |
| Pamięć operacyjna | Min. 128GB RDIMM DDR5 4800 MT/s w modułach pamięci o pojemności min. 32 GB każdy  Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB. |
| Sloty rozszerzeń | Min. 3 aktywnych gniazd PCI-Express generacji 5, x16 (szybkość slotu – bus width). 1x gniazda pełnej wysokości (full height) 2x gniazda połówkowej wysokości gotowe do obsadzenia kartami z portami zewnętrznymi.  Dwa sloty OCP 3.0 możliwe do obsadzenia poprzez kontrolery sprzętowe dla dysków lub karty sieciowe w dowolnej konfiguracji. |
| Dysk twardy | Serwer bez klatkowy z możliwością rozbudowy/rekonfiguracji w przyszłości serwera do 10 dysków typu Hot Swap, SAS/SATA/SSD/NVMe, 2,5” montowane z przodu obudowy.  W przypadku braku opcji rozbudowy/rekonfiguracji o dodatkowe zatoki dyskowe, serwer standardowo wyposażony w minimum 10 zatoki dyskowe SFF gotowe do instalacji dysków SAS/SATA/SSD/NVMe 2,5”typu Hot Swap.  Zainstalowane min. 2szt. dysków SSD NVMe 960GB nie zajmujące wnęk na dyski twarde pracujące w konfiguracji ze sprzętowym  RAID 1. |
| Kontroler | Serwer wyposażony w kontroler software dla dysków SATA, obsługujący poziomy: RAID 0, 1, 5, 10.  Możliwość zastosowania/wymiany kontrolera na kontroler sprzętowy wyposażony w min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę napędów dyskowych SSD/SATA/SAS/NVMe.  Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie. |
| Interfejsy sieciowe | Jedna dwuportowa karta 10Gb Base-T oparta o chipset BMC57416. |
| Karta graficzna | Zintegrowana karta graficzna |
| Porty | 5 x USB, z czego min 4szt w wersji USB 3.2 oraz jeden port USB 2.0  1x VGA  Możliwość rozbudowy/rekonfiguracji o:  - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express  - cyfrowy port video ( Display Port lub HDMI), bez użycia przejściówek z portu VGA lub USB 8 |
| Zasilacz | 2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1000W. |
| Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug |
| Diagnostyka | Możliwość zainstalowania elektronicznego panelu diagnostycznego dostępnego z przodu serwera pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy, temperaturze. |
| Bezpieczeństwo | Serwer wyposażony w moduł TPM 2.0. |
| Karta/moduł zarządzający | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:  · monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe  · praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP  · dostęp do karty zarządzającej poprzez  - dedykowany port RJ45 z tyłu serwera lub  - przez współdzielony port zintegrowanej karty sieciowej serwera  dostęp do karty możliwy  - z poziomu przeglądarki webowej (GUI)  - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)  - z poziomu skryptu (XML/Perl)  - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)  · wbudowane narzędzia diagnostyczne  · zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego  · obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie  · wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników  · przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)  · uwierzytelnianie oprogramowania sprzętowego PCIe z protokołem bezpieczeństwa i modelem danych (SPDM) zapewnia integralność komponentu  · obsługa zdalnego serwera logowania (remote syslog)  · wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów  · mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie  · funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności  · monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji  · konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)  · zdalna aktualizacja oprogramowania (firmware)  · zarządzanie grupami serwerów, w tym:  - tworzenie i konfiguracja grup serwerów  - sterowanie zasilaniem (wł/wył)  - ograniczenie poboru mocy dla grupy (power capping)  - aktualizacja oprogramowania (firmware)  - wspólne wirtualne media dla grupy  · możliwość równoczesnej obsługi przez 6 administratorów  · autentykacja dwuskładnikowa (Kerberos)  · wsparcie dla Microsoft Active Directory  · obsługa SSL i SSH  · enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli  · wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API  · wsparcie dla Integrated Remote Console for Windows clients  · możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) |
| Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Serwer jest dostarczany bez Systemu operacyjnego  Zapewnia wsparcie dla:  Microsoft Windows Server 2019, 2022  Ubuntu 22.04 LTS  Red Hat Enterprise Linux (RHEL) 8.6 oraz 9.0  SUSE Linux Enterprise Server (SLES) 15 SP4  VMware ESXi 7.0 U3, 8.0 |
| Wsparcie techniczne | Minimum 24-miesięczna gwarancja producenta na części, robociznę i naprawę w miejscu instalacji typu On-Site z 4-godzinnym czasem reakcji przez całą dobę (przybycie na miejsce). 15-minutowy czas reakcji na zdarzenia krytyczne przez całą dobę, 7 dni w tygodniu.  Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń. |
| Inne | Wymagane jest, aby sprzęt był produkowany zgodnie z normami ISO 9001 oraz ISO 14001 lub równoważnymi oraz posiadał deklarację zgodności CE. |

1. **Macierz dyskowa – 1 szt.**

Minimalne wymagania dostarczanej macierzy dyskowej:

**Macierz All-flash NAS 44TB – 1szt**

|  |  |  |
| --- | --- | --- |
| Lp | Cecha | Opis Wymagań |
|  | Obudowa | Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Maksymalna wyskość obudowy to 2U. |
|  | Kontrolery dyskowe | Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active-active. Kontrolery nie mogą pracować w trybie active-passive. Macierz musi umożliwiać rozbudowę do co najmniej 4 kontrolerów. Wszystkie kontrolery muszą być zarządzane z jednego interfejsu graficznego. Nie dopuszcza się zastosowania wirtualizatora do połączenia 4 kontrolerów. |
|  | Zasilanie | Oferowane urządzenie musi być przystosowane do zasilania z sieci AC oraz wyposażone w kable zasilające PDU. Macierz musi być wyposażona w zdublowany, redundantny system zasilania, umożliwiający prawidłową, nieprzerwaną pracę urządzenia w przypadku awarii dowolnego pojedynczego źródła zasilania. |
|  | Redundancja | Macierz nie może posiadać pojedynczego punktu awarii (SPOF), który powodowałby brak dostępu do danych. Wszystkie krytyczne komponenty takie jak kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo. |
|  | Wymagana przestrzeń | Fizyczna przestrzeń dyskowa zbudowana tylko i wyłącznie za pomocą SSD SAS. Przestrzeń użytkowa po zbudowaniu grupy RAID 6 z 1 dyskiem hot-spare lub przestrzenią hot-spare równą pojemności 1 dysku musi wynosić min 44 TB. Ze względów wydajnościowych oraz niezawodnościowych całej macierzy pojemność RAW pojedynczego dysku nie może być większa niż 4 TB. 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.  Oferowana macierz musi umożliwiać rozbudowę do min 100 dysków tego samego typu, czyli SSD SAS bez konieczności klastrowania oferowanej macierzy z dodatkowymi kontrolerami. Nie dopuszcza zastosowania się chipsetu QLC w dyskach SSD SAS. Macierz nie może obsługiwać dysków HDD. |
|  | Zabezpieczenia dyskami SPARE | Możliwość definiowania przez administratora dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej. |
|  | Pamięć Cache | Co najmniej 128GB pamięci cache na całą macierz (dwa kontrolery). Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin. |
|  | Dostępne interfejsy front-end | Razem kontrolery muszą udostępnić minimum 8 portów 1G Eth RJ45 oraz min 8 portów 10Gb Eth z wkładkami optycznymi. Wymagana możliwość rozbudowy o 8 portów 25G Eth tylko poprzez dodanie nowych kart sieciowych. |
|  | Obsługiwane protokoły | Wymagane wsparcie dla NFS, CIFS. Nie dopuszcza się spełnienia wymogu poprzez zastosowanie główki/gateway NAS. |
|  | Obsługiwane typy zabezpieczenia RAID | Kontrolery wyposażone w funkcjonalność konfiguracji poziomu RAID 6 lub równoważnego tolerującego jednoczesną awarię 2 dysków. |
|  | Thin Provisioning | Wymagana funkcjonalność tworzenia file system’ów o pojemności większej niż zajmowana fizyczna przestrzeń dyskowa (ang. ThinProvisioning). Wymagana możliwość zwiększania pojemności file system’ów w sposób online. |
|  | Multi-tenancy | Wymagana możliwość logicznego podziału macierzy na wiele wirtualnych/logicznych systemów z dedykowanymi portami logicznymi, użytkownikami oraz uprawnieniami. Użytkownik danego wirtualnego/logicznego systemu nie może mieć dostępu do file system’u z innego wirtualnego/logicznego systemu. |
|  | Zarządzanie | Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagany także dostęp do CLI. Zarządzanie poprzez min 2 porty 1Gb Eth typu management.  Wymagane jest stałe monitorowanie stanu macierzy w tym monitorowanie wydajności obiektów takich jak:  - cała macierz  - kontrolery  - porty front-end  - porty logiczne  - dyski  - file systemy  - hosty  - CPU  Pod kątem parametrów takich jak:  - operacje wejścia/wyjścia IOPS  - przepustowość (KB/s lub MB/s)  - czas odpowiedzi (latency)  - średnie użycie CPU w % dla kontrolerów  Wymagana możliwość monitorowania stanu żywotności dysków SSD SAS. Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI macierzy do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych w formie wykresów graficznych.  Wymagana możliwość konfigurowania zasobów macierzy.  Wymagana możliwość tworzenia polityk logowania.  Wymagane wsparcie multi-factor authentication do logowania się do macierzy. |
|  | Kopie wewnątrz macierzy | Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych. Snapshoty muszą być wykonywanie w technologii ROW (Redirect On Write). Macierz musi umożliwiać utworzenie min 4000 snapshotów.  Wymagana możliwość prezentacji folderu ze snapshotami w ramach udziału CIFS pod kątem przywracania pojedynczych plików.  Wymagana możliwość przywrócenia pojedynczego pliku ze snapshota do file system’u w ramach operacji macierzy na poziomie CLI.  Wymagana możliwość tworzenia harmonogramu wykonywania snapshotów. Wymagana możliwość zabezpieczenia snapshotów przed modyfikacją lub usunięciem przez wybrany okres czasu pod kątem szybkiego przywrócenia danych w przypadku ataku ransomware. |
|  | Replikacja file system’ów | Możliwość zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym z wykorzystaniem portów IP. Funkcjonalność ta nie może wpływać na obciążenie serwerów podłączonych do macierzy.  Macierz musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60min) lub konkretnych okien czasowych (np. w każdą sobotę o godz 20:00). |
|  | Kontrola zasobów plikowych | 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 na wystawionych udziałach CIFS/NFS poprzez wykluczenie ich konkretnych rozszerzeń. Wymagana także możliwość wskazania rozszerzeń które mogą być zapisywane.  Wymagana możliwość nadawania uprawnień do określonych operacji dla wybranych użytkowników na udziałach CIFS/NFS.  Wymagana możliwość ograniczenia dostępu do udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp. |
|  | Ochrona zasobów plikowych | Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem na poziomie całego file system’u (WORM).  Wymagana możliwość podłączenia serwera z oprogramowaniem antywirusowym celem skanowania plików wykorzystywanych przez użytkowników na zasobach wystawionych przez macierz protokołem CIFS. |
|  | Wydajność | Model macierzy w oferowanej konfiguracji w teście wydajnościowym musi osiągnąć min 1800 MB/s przy następujących parametrach:  - Zapełnienie macierzy – powyżej 70% fizycznej pojemności,  - Protokół: NFSv3,  - Porty: 10G,  - Read: 70%,  - Write: 30%,  - typ workloadu: Random,  - wielkość plików: 64KB,  - Latency: <3ms,  - RAID 6 lub równoważny |
|  | Serwisowalność | Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych.  Macierz przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączania.  Macierz musi umożliwiać zdalne zarządzanie.  Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z legalnego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub partnera serwisowego lub wykonawcy. |

1. **Serwerowe systemy operacyjne i oprogramowanie bezpieczeństwa**
   1. **System operacyjny – 1 szt.**

Zamawiający aktualnie korzysta z oprogramowania typu Microsoft Windows Server 2022 Standard i wymagana dostarczenia licencji na oprogramowanie Microsoft Windows Server 2022 Standard 64-bit PL lub nowszy + 80 licencji CAL User lub równoważny serwerowy system operacyjny.

**Opis równoważności oprogramowania**

Przez oprogramowanie równoważne Zamawiający rozumie oprogramowanie spełniające następujące warunki poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Wszystkie elementy systemu oraz jego licencja pochodzą od tego samego producenta.
2. Wymaga się dostarczenia odpowiedniej liczby licencji dla serwerów, 2 i 1- procesorowych, posiadających min 12 rdzeni,
3. Jeżeli wymagane jest posiadanie licencji dostępowych, należy dostarczyć licencję dla odpowiedniej liczby użytkowników.
4. Licencja na SSO zapewnia uruchomienie systemu operacyjnego w środowisku fizycznym i min. 2 w środowisku wirtualnym za pomocą wbudowanego mechanizmu wirtualizacji, bez konieczności zakupu dodatkowych licencji.
5. SSO posiada graficzny interfejs użytkownika umożliwiający jego obsługę przy pomocy klawiatury i myszy.
6. Obsługa do 48 TB RAM
7. SSO musi posiadać obsługę zdalnego pulpitu zgodnego z protokołem RDP
8. Możliwość uruchomienia posiadanego, skonfigurowanego i używanego przez Zamawiającego oprogramowania do backupu, aktualnie zainstalowanego na systemie operacyjnym Windows.
9. Pełna współpraca z procesorami o architekturze 64 bit
10. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym
11. SSO zapewniający natywne wsparcie dla środowiska .NET Framework 4.x
12. System operacyjny musi wspierać pracę domenową.
13. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory
14. Zawarta możliwość uruchomienia roli serwera DNS
15. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory
16. Posiada wbudowaną zaporę sieciową (firewall) dla połączeń przychodzących i wychodzących z systemu.
17. Interfejsy użytkownika dostępne w wielu językach do wyboru - w tym polskim i angielskim,
18. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
19. Możliwość dokonywania bezpłatnych aktualizacji i poprawek
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
21. Zabezpieczenie hasłem dostępu do systemu, konta i profilu użytkowników,
22. Mechanizmy logowania w oparciu o login i hasło,
23. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości współbieżnej (ang. Simultaneous Multi-Threading, SMT).
24. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
25. pozwalają na zmianę rozmiaru w czasie pracy systemu,
26. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
27. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
28. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
29. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
30. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
31. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
32. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
33. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC
34. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe).
35. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie minimum 2 aktywnych środowisk wirtualnych systemów operacyjnych.
36. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
37. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
38. Dostarczone oprogramowanie musi być fabrycznie nowe.

Ogólne zasady oceny równoważności

1. W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne (dotyczy równoważności we wszystkich wskazanych powyżej przypadkach) nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.
2. Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych, jako rozwiązania referencyjne, po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.
3. Wykonawca zobowiązany jest podać w ofercie co najmniej nazwę producenta, nazwę oferowanego Oprogramowania, identyfikator Oprogramowania nadawany przez jego producenta, rodzaj licencji (według oznaczenia producenta), w sposób umożliwiający Zamawiającemu jednoznaczną identyfikację i weryfikację zaoferowanego Oprogramowania oraz udowodnić, że oferowane rozwiązanie spełnia wskazane przez Zamawiającego kryteria stosowane w celu oceny równoważności.
4. Zamawiający nie dopuszcza dostarczenia licencji dla produktów równoważnych w formie upgradu czy licencji czasowej.
5. Zamawiający nie dopuszcza zaoferowania subskrypcji licencyjnej opartej o rozwiązania chmurowe.
6. W przypadku błędnego działania środowiska lub wykrytych niezgodności pod kątem spełnienia warunków OPZ po instalacji oprogramowania równoważnego Zamawiający ma prawo odstąpić od umowy.

Co do pozostałych równoważności to Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych, jako rozwiązania referencyjne, po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.

Jeżeli Wykonawca chce zaproponować rozwiązanie równoważne to musi to jasno wynikać z oferty, przy czym ma również udowodnić, że oferowane rozwiązanie spełnia wskazane przez Zamawiającego kryteria stosowane w celu oceny równoważności.

* 1. **Oprogramowanie do Wirtualizacji**

|  |  |
| --- | --- |
| **LP.** | **Wymagania funkcjonalno-techniczne (minimalne)** |
| 1 | Licencja na oprogramowanie musi pozwalać na pełne wykorzystanie sprzętowych zasobów serwera |
| 2 | Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych |
| 3 | Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. |
| 4 | Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 320 logicznych wątków oraz do 4TB pamięci fizycznej RAM. |
| 5 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-64 procesorowych. |
| 6 | Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB |
| 7 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 1 TB pamięci operacyjnej RAM. |
| 8 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-10 wirtualnych kart sieciowych. |
| 9 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć co najmniej 4 porty szeregowe i 3 porty równoległe i 20 urządzeń USB. |
| 10 | Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. |
| 11 | Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. |
| 12 | Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade).  Licencjonowanie nie może odbywać się w trybie OEM. |
| 13 | Rozwiązanie musi umożliwiać poprawne zainstalowanie następujących systemów operacyjnych: Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES 11, SLES 10, SLES 9, SLES 8, RHEL 6, RHEL 5, RHEL 4, RHEL 3, Solaris 11,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 6.5, NetWare 6, NetWare 5, OEL 4, OEL 5, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu 12.04, SCO OpenServer, SCO Unixware, Mac OS X |
| 14 | Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. |
| 15 | Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. |
| 16 | Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. |
| 17 | Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.  Z możliwością wysyłania maila o wykonanej kopii bezpieczeństwa |
| 18 | Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. |
| 19 | Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. |
| 20 | Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. |
| 21 | Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. |
| 22 | Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione na nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. |
| 23 | System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. |
| 24 | Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. |
| 25 | Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). |
| 26 | Należy dostarczyć licencję obsługującą 3 serwery po 2 procesory. |

1. **Zasilanie awaryjne – UPS – 1 szt.**

|  |  |
| --- | --- |
| Parametr | Charakterystyka (wymagania minimalne) |
| Moc pozorna | Min. 6000VA |
| Moc rzeczywista | Min. 5400Wat |
| Obudowa | Obudowa Rack o wysokości max 3U |
| Liczba gniazd | Liczba wyjść C13: min. 8, C19: min. 2 |
| Złącze wejściowe | Połączenia kablowe/stałe |
| Kształt fali na wyjściu | Fala sinusoidalna |
| Zakres częstotliwości wejściowych | 40-70 Hz |
| Wyjściowy współczynnik mocy | 0,9 |
| Czas podtrzymania | Zasilacz przy obciążeniu 3500Wat musi podtrzymywać min. 6 minut |
| Protokół | SNMP |
| Karta sieciowa | Zasilacz musi mieć wbudowaną kartę sieciową |
| Bypass | Wewnętrzny bypass zapewnia ciągłość pracy w przypadku awarii zasilacza UPS |
| Parametry znamionowe akumulatora | 12 V / 5 Ah |
| Wymiana akumulatorów | Wewnętrzne akumulatory, które można wymieniać bez przerywania pracy i moduły akumulatorowe o większej pojemności (EBM) |
| Wyświetlacz | Zasilacz musi posiadać wyświetlacz graficzny LCD |
| Interfejs komunikacyjny | W zestawie musi być karta sieciowa ethernet. |
| Gwarancja | 1. lat gwarancji producenta |

1. **Szkolenia specjalistyczne**

Zamówienie obejmuje szkolenia z wdrażanych rozwiązań w ramach zamówienia

1. Zamawiający wymaga aby Wykonawca zorganizował i przeprowadził szkolenie w siedzibie Zamawiającego.
2. Szkolenie ma obejmować dostarczane oprogramowania i urządzenia.
3. Warsztaty mają odbyć się w formie stacjonarnej.
4. Zamawiający wymaga aby usługa została zrealizowana w terminie realizacji zamówienia po dostarczeniu i wdrożeniu urządzeń oraz oprogramowania. Dokładny termin zostanie ustalony zgodnie z procedurą przewidzianą we wzorcu umowy.
5. Zamawiający wymaga przeszkolenia w formie warsztatów 2 uczestników, z tym że ilość jest szacunkowa, co nie powinno wpływać na koszty.
6. Zamawiający wymaga aby w trakcie warsztatów realizowane były ćwiczenia opisujące codzienną pracę administracyjną z wdrożonym rozwiązaniem, rozwiązywaniem problemów, procedurę aktualizacji rozwiązania oraz rozbudowy o dodatkowe widoki i kanały napływu danych.
7. Zamawiający wymaga aby warsztaty zamykały się w ramach czasowych 2 dni roboczych (2x 7 godz.)
8. Zamawiający wymaga aby warsztaty kończyły się potwierdzeniem uczestnictwa w formie certyfikatu potwierdzającego odbyte szkolenie.