*Numer referencyjny nadany sprawie przez Zamawiającego: ZZP.261.33.2020* **Załącznik nr 3 do SIWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA (PARAMETRY TECHNICZNE)**

# Serwer do pracy w klastrze – 2 szt.

|  |  |
| --- | --- |
| **Nazwa komponentu, parametru lub cechy** | **Opis wymagań lub parametrów minimalnych** |
| Zastosowanie | Serwery rack 19’’ dedykowane do pracy w klastrze (2 sztuki o identycznej konfiguracji sprzętowej) |
| Ilość procesorów | 2 szt. 8-rdzeniowe |
| Procesor | Parametr wydajności – procesor powinien osiągać w teście wydajności PassMark PerformanceTest (https://www.cpubenchmark.net/), wynik co najmniej **23000** punktów Passmark CPU Mark |
| Obudowa | Rack 19” typu hotplug o wysokości max 1U |
| Zasilanie | Redundantne, zasilacze hot plug o mocy optymalnej do zasilenia serwera wyposażonego w komplet dysków i kart rozszerzeń |
| Kontroler RAID | Sprzętowy, pamięć cache 2 GB, umożliwiający zbudowanie macierzy RAID na poziomach: 0,1,5,6,10,50,60 |
| Pamięć | 24 sloty, zainstalowane 4x 64 GB pamięci DDR4 3200 MHz |
| Zabezpieczenie pamięci | Memory Rank Sparing, Memory Mirror, Failed DIMM Isolation, Memory Thermal Throttling |
| Obsługa dysków | 8 slotów na dyski 2,5” typu SATA, SAS, SSD, SED, transfer 12 Gb/s |
| Zamontowane dyski typ 1 | 2x 600 GB SAS 12Gb/s 15k RPM |
| Zamontowane dyski typ 2 | 4x 1,6 TB 2,5" SSD Mix Use SAS |
| Karta sieciowa | 4 gniazda RJ-45 GbE, w tym dwa interfejsy sieciowe 10Gb Ethernet SFP+ |
| Porty komunikacyjne | USB 3.0 – 4 szt., , 2 x VGA, port zarządzania serwerem |
| Wspierane systemy operacyjne | Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2012, Microsoft Windows 2012 R2, Microsoft Windows 2016, Microsoft Windows 2019 x64 |
| Dokumentacja | Dokumentacja użytkownika w języku polskim |
| Dodatkowe elementy wyposażenia | Przewody zasilające, szyny montażowe, uchwyty adaptujące, ramka zamykana na kluczyk, chroniąca dyski przed nieuprawnionym dostępem. |
| Karta zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika * możliwość podmontowania zdalnych wirtualnych napędów * wirtualną konsolę z dostępem do myszy, klawiatury * wsparcie dla IPv6 * wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer * integracja z Active Directory * możliwość obsługi przez sześciu administratorów jednocześnie * możliwość podłączenia lokalnego poprzez złącze RS-232. * możliwość zarządzania bezpośredniego poprzez złącze micro USB umieszczone na froncie obudowy * monitorowanie zużycia dysków SSD * możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi |
| Gwarancja | 3-letnia gwarancja w miejscu użytkowania w reżimie NBD (w następnym dniu roboczym), uszkodzone dyski pozostają u Zamawiającego |
| Dostęp do oprogramowania | Dostęp do aktualnych sterowników zainstalowanych w serwerze urządzeń, realizowany przez podanie modelu lub nr seryjnego serwera, na dedykowanej przez producenta stronie internetowej. |
| Wymagania dodatkowe | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001:2015 i posiadać deklarację CE. |

# Urządzenie UPS wraz z dodatkowym modułem baterii – 1 kpl.

Zestaw składający się z trzech wzajemnie kompatybilnych elementów dedykowanych do współpracy jako jeden komplet.

## UPS – 1 szt.

|  |  |
| --- | --- |
| **Nazwa komponentu, parametru lub cechy** | **Opis wymagań lub parametrów minimalnych** |
| Typ | Zasilacz awaryjny z kartą zarządzającą oraz czujnikami |
| Mocowanie | Rack 19”z możliwością transformacji do Tower |
| Moc wyjściowa | 2.7KW / 3.0 kVA |
| Napięcie wyjściowe | 230V 50/60Hz |
| Napięcie wejściowe | 140 - 280 V – 50/60 Hz |
| Topologia/typ przebiegu | Line Interactive /Sinusoida |
| Czas przełączania | Do 4 ms |
| Gniazda wyjściowe zasilające | 3 sterowalne grupy minimum 8 gniazd EC 320 C13, 1 gniazdo IEC 320 C19 |
| Pozostałe gniazda | RJ45 LAN, USB, SERIAL, Smart Slot |
| Obsługa | Wyświetlacz statusu LCD, konsola sterownicza z poziomu urządzenia, zarządzanie grupami gniazd wyjściowych z poziomu urządzenia bądź oprogramowania |
| Sygnalizacja optyczna | Wyświetlacz statusu, wskaźniki: praca online, wymiana baterii, przeciążenie. |
| Sygnalizacja dźwiękowa | Alarm przy zasilaniu z akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora |
| Interfejsy | Karta zarządzająca SNMP z portami USB, LAN, I/O, czujnik temperatury, czujnik wilgotności, złącze dodatkowego akumulatora |
| Oprogramowanie | Dostęp przez przeglądarkę, Telnet, SSH, obsługa czujnika temperatury, zarządzanie akumulatorami, monitorowanie i sterowanie, bezpieczne zamykanie systemu operacyjnego |
| Wyposażenie | Szyny montażowe (szyny) do szafy rack, kabel do sygnalizacji RS-232, czujnik temperatury I wilgotności, zestaw do transformacji w urządzenie wolnostojące typu TOWER, karta zarządzająca z monitorowaniem warunków otoczenia |
| Bezpieczeństwo | Ochrona hasłem, poziomy dostępu: administrator, użytkownik urządzenia, użytkownik z prawem tylko do odczytu i użytkownik tylko z dostępem sieciowym |
| Inne | Zdalny restart |
| Typ akumulatora | Bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny |
| Gwarancja | 24 miesiące w miejscu instalacji |

## DODATKOWA BATERIA – 1 szt.

|  |  |
| --- | --- |
| **Nazwa komponentu, parametru lub cechy** | **Opis wymagań lub parametrów minimalnych** |
| Zastosowanie | Zewnętrzny pakiet bateryjny rozszerzający możliwości zasilacza awaryjnego |
| Mocowanie | Rack 19” z możliwością transformacji do Tower |
| Wartość napięcia na wyjściu | 120 V |
| Typ akumulatora | kwasowo-ołowiowy |
| Oczekiwana żywotność akumulatora | 3-5 lat |
| Pojemność Akumulatora | 1200 VAh |
| Wyposażenie | Szyny montażowe do szaf rack 19”, zestaw do transformacji w urządzenie wolnostojące typu TOWER |
| Okres gwarancji | 24 miesiące na naprawę lub wymianę w miejscu instalacji |

## PANEL OBEJŚCIA SERWISOWEGO DLA ZASILACZA – 1 szt.

|  |  |
| --- | --- |
| **Nazwa komponentu, parametru lub cechy** | **Opis wymagań lub parametrów minimalnych** |
| Zastosowanie | Panel obejścia serwisowego o wysokim stopniu niezawodności z zabezpieczeniem przed przeciążeniem na wyjściu |
| Zasada pracy | Najpierw zwarcie, potem rozwarcie |
| Mocowanie | Rack 19” z możliwością montażu do urządzenia |
| Złącza wyjściowe | 4 szt. IEC 60320 C19 |
| Napięcie wyjściowe | 230 V |
| Nominalne napięcie wejściowe | 230 V |
| Typ gniazda wejściowego | Hard wire 3-wire (1P + N + E) |
| Wydajność przy pełnym obciążeniu na wyjściu | 99% |
| Zabezpieczenie przed przeciążeniem na wyjściu | TAK |
| Maksymalny łączny pobór prądu na wyjściu | 32A |
| Maksymalny prąd wejściowy | 32A |
| Maksymalny prąd linii | 32A |
| Okres gwarancji | 24 miesiące w miejscu instalacji |

# Urządzenie UTM firewall – 1 szt.

Dostawa urządzenia UTM firewall kompatybilnego z posiadanym przez Zamawiającego urządzeniem Fortigate 80E w celu utworzenia klastra pozwalającego na zapewnienie wysokiego poziomu bezawaryjności.

Przez urządzenie kompatybilne Zamawiający rozumie urządzenie spełniające poniższe wymagania minimalne:

|  |  |
| --- | --- |
| **Nazwa parametru lub cechy** | **Opis wymagań lub parametrów minimalnych** |
| Wymagania Ogólne | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. |
|  | System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. |
|  | W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu. |
|  | System musi wspierać IPv4 oraz IPv6 w zakresie: |
|  | • Firewall. |
|  | • Ochrony w warstwie aplikacji. |
|  | • Protokołów routingu dynamicznego. |
|  |  |
| Redundancja, monitoring i wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. |
|  | 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. |
|  | 3. Monitoring stanu realizowanych połączeń VPN. |
|  | 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |
|  |  |
| Interfejsy, Dysk, Zasilanie | 1. System realizujący funkcję Firewall musi dysponować minimum:   * 14 portami Gigabit Ethernet RJ-45. * 2 gniazdami SFP 1 Gbps.   2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.  3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.  4. System musi być wyposażony w zasilanie AC. |
|  |  |
| Parametry wydajnościowe | 1. W zakresie Firewall’a obsługa nie mniej niż 1.3 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.  2. Przepustowość Stateful Firewall: nie mniej niż 4 Gbps dla pakietów 512 B.  3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 900 Mbps.  4. Wydajność szyfrowania IPSec VPN nie mniej niż 2.5 Gbps.  5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 450 Mbps.  6. Wydajność skanowania ruchu typu z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps.  7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 130 Mbps. |
|  |  |
| Funkcje Systemu Bezpieczeństwa | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: |
|  | 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. |
|  | 2. Kontrola Aplikacji. |
|  | 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. |
|  | 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. |
|  | 5. Ochrona przed atakami - Intrusion Prevention System. |
|  | 6. Kontrola stron WWW. |
|  | 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. |
|  | 8. Zarządzanie pasmem (QoS, Traffic shaping). |
|  | 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). |
|  | 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. |
|  | 11. Analiza ruchu szyfrowanego protokołem SSL. |
| Polityki, Firewall | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. |
|  | 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: |
|  | • Translację jeden do jeden oraz jeden do wielu. |
|  | • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. |
|  | 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |
|  |  |
| Połączenia VPN | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: |
|  | • Wsparcie dla IKE v1 oraz v2. |
|  | • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). |
|  | • Obsługa protokołu Diffie-Hellman grup 19 i 20. |
|  | • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. |
|  | • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. |
|  | • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. |
|  | • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. |
|  | • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. |
|  | • Mechanizm „Split tunneling” dla połączeń Client-to-Site. |
|  | 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: |
|  | • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. |
|  | • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. |
|  |  |
| Routing i obsługa łączy WAN | 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:  · Routingu statycznego oraz Policy Based Routingu. |
|  | · Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |
|  | 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. |
|  |  |
| Zarządzanie pasmem | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. |
|  | 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. |
|  | 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |
|  |  |
| Ochrona przed malware | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). |
|  | 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: ZIP, RAR. |
|  | 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). |
|  | 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. |
|  | 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |
|  |  |
| Ochrona przed atakami | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. |
|  | 2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |
|  | 3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. |
|  | 4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. |
|  | 5. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. |
|  | 6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |
|  |  |
| Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. |
|  | 2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. |
|  | 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. |
|  | 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. |
|  | 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |
|  |  |
| Kontrola WWW | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. |
|  | 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance. |
|  | 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. |
|  | 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. |
|  | 5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. |
|  | 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. |
|  |  |
| Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: |
|  | • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. |
|  | • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. |
|  | • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. |
|  | 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. |
|  | 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |
|  |  |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. |
|  | 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. |
|  | 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. |
|  | 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. |
|  | 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. |
|  | 6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |
|  |  |
| Logowanie | 1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. |
|  | 3. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. |
|  | 4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. |
|  | 5. Musi istnieć możliwość logowania do serwera SYSLOG. |
|  |  |
| Certyfikaty | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: |
|  | • ICSA lub EAL4 dla funkcji Firewall. |
|  | • ICSA lub NSS Labs dla funkcji IPS. |
|  | • ICSA dla funkcji IPSec VPN. |
|  | • ICSA dla funkcji SSL VPN. |
|  |  |
| Serwisy i licencje | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: |
|  | • Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), analiza typu Sandbox, antyspam, web filtering, bazy reputacyjne adresów IP/domen  na okres 36 miesięcy. |
|  |  |
| Gwarancja oraz wsparcie | System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
|  |  |
| Rozszerzone wsparcie serwisowe | System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym (NBD) od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy. |

# Wsparcie dla urządzenia Fortigate 80E – 24 miesiące

Zamawiający oczekuje przedłużenia trwających obecnie usług wsparcia (do dnia 2021.03.17) dla posiadanego i eksploatowanego urządzenia firmy Fortinet Fortigate 80E ze wsparciem w trybie 24x7 FortiCare FortiGuard UTM Protection na okres 24 miesięcy.

# Switch 24-portowy – 2 szt.

|  |  |  |
| --- | --- | --- |
| **Nazwa parametru lub cechy** | **Opis wymagań lub parametrów minimalnych** |  |
| Wymagania Ogólne | Zamawiający jest w posiadaniu rozwiązania FortiGate, model 80E. W ramach rozbudowy istniejącego systemu, której celem jest przeniesienie mechanizmów bezpieczeństwa na warstwę dostępową, wymaganym jest dostarczenie przełącznika współpracującego z istniejącym rozwiązaniem Fortigate w zakresie opisanym w sekcjach: *"Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC"* oraz *"Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa".* |  |
| Parametry fizyczne | * Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. * Zasilanie AC 230V. * Wbudowany redundantny zasilacz. * Maksymalny pobór mocy: 20 W. * Minimalny zakres temperatury pracy: 0-50ᵒC. |  |
| Interfejsy sieciowe | Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:   * 24 porty GE RJ-45. * 4 porty GE, SFP. |  |
| Zarządzanie | * Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania. * Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. * Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). * Wsparcie dla SNMP w wersjach 1-3 * Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. * Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. * Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. * Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). * Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. * Funkcja definiowania ról administratorów przydzielających tryb dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. * Automatycznie wykonywane rewizje konfiguracji |  |
| Parametry wydajnościowe | * Przepustowość urządzenia - min. 56 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 82 Mps. * Tablica adresów MAC o pojemności co najmniej 16 k wpisów. * Opóźnienie wprowadzane przez przełącznik - poniżej 1 mikrosekund |  |
| Wymagane funkcje | * Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. * Obsługa Jumbo Frames. * Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). * Agregacja portów zgodna ze standardem 802.3ad. * Obsługa co najmniej 4000 VLANów, zgodna ze standardem 802.1Q. * Wsparcie dla Private VLAN. * Obsługa routingu statycznego. * Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP. * Port-mirroring. * Uwierzytelnianie 802.1x na poziomie portu. * Uwierzytelnianie 802.1x w oparciu o adres MAC. * W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN). * W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. * W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. * Obsługa protokołu sFlow. |  |
| Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC | 1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:  * Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. * Centralne zarządzanie sieciami VLAN. * Rozpoznawanie urządzeń uzyskujących dostęp do sieci. * Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. * Obsługa białych i czarnych list adresów MAC. * Wykrywanie aplikacji komunikujących się w sieci. * W przypadku gdy do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC wymagane są licencje, producent zobowiązany jest je dostarczyć .  1. Musi być możliwe redundantne połączenie z elementami zarządzającymi. |  |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa | * Stateful firewall, umożliwiający kontrolę pomiędzy sieciami VLAN. * Routing statyczny i dynamiczny (co najmniej OSPF). * Policy Based Routing. |  |
| Gwarancja i wsparcie | System musi być objęty serwisem gwarancyjnym producenta **przez okres** **36 miesięcy**, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne **w trybie** **24x7**. |  |

# Oprogramowanie

Zamawiający wymaga dostawy następujących licencji oprogramowania do serwerów (pozycja 1):

|  |  |  |
| --- | --- | --- |
|  | **System operacyjny** | Licencja wieczysta Windows Serwer 2019 DataCenter,  obejmująca wszystkie rdzenie procesorów serwera, rodzaj licencji: elektroniczna, wieczysta. |
|  | **Licencje dostępowe** | Microsoft Windows Server 2019 10 CALs Device, 1 licencja na 10 urządzeń, rodzaj licencji: elektroniczna, wieczysta, per urządzenie |
| 1. **A** | **Oprogramowanie do tworzenia kopii bezpieczeństwa** | Veeam Backup Essentials Enterprise 2 socket Bundle 1yr support  V-ESSENT-VS-P0000-00 |
| 1. **B** | **Wsparcie techniczne dla oprogramowania do tworzenia kopii bezpieczeństwa** | 2 additional years of Basic maintenance prepaid for Veeam Backup Essentials Enterprise 2 socket bundle V-ESSENT-VS-P02YP-00 |

Zgodnie z art. 29 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843, ze zm.) (dalej jako: Ustawa PZP) mając na uwadze specyfikację przedmiotu zamówienia i fakt że zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń, w każdym przypadku, w którym wskazano lub użyto w niniejszym dokumencie oraz załącznikach odpowiednio: znaków towarowych, patentów lub pochodzenia materiałów należy rozumieć, że zamawiający dopuszcza stosowanie materiałów równoważnych o porównywalnych (nie gorszych) parametrach technicznych, eksploatacyjnych i użytkowych niż te, które wskazano a wskazaniu takiemu towarzyszą wyrazy „lub równoważny”.

Ponadto zgodnie z art. 30 ust 4 Ustawy PZP ilekroć w niniejszym dokumencie lub załącznikach zamawiający odnosi się do określonych norm, aprobat, specyfikacji technicznych lub systemów Zamawiający dopuszcza rozwiązania równoważne z opisywanym a odniesieniu takiemu towarzyszą wyrazy „lub równoważne”..

Wykonawca, który powołuje się na rozwiązania równoważne jest zobowiązany wykazać, że oferowane przez niego oprogramowanie, spełnia wymagania określone przez Zamawiającego.

Ciężar udowodnienia, że materiał (wyrób) jest równoważny w stosunku do wymogu określonego przez Zamawiającego spoczywa na składającym ofertę.

Dostarczane licencje muszą być przeznaczone do użytku na terenie Rzeczpospolitej Polskiej.

Wykonawca w zakresie przekazanego oprogramowania/licencji zgodnie z umową zawartą w wyniku niniejszego postepowania, przedstawi Zamawiającemu potwierdzenie legalności zakupionego produktu celem ewentualnego przedstawienia podmiotowi, który może na żądanie zwrócić się do Zamawiającego o potwierdzenie nabycia wspomnianego przedmiotu Umowy z legalnego źródła.

Dopuszcza się zaoferowanie produktu równoważnego do licencji oprogramowania do tworzenia kopii bezpieczeństwa (oznaczonego numerem 3A oraz 3B). Oprogramowanie równoważne musi zapewniać opisaną poniżej funkcjonalność. Warunki licencji oprogramowania równoważnego w każdym aspekcie licencjonowania nie mogą być gorsze niż licencje oprogramowania.

W przypadku zaoferowania oprogramowania równoważnego Wykonawca jest zobowiązany do wskazania w ofercie, że funkcjonalność oferowanego oprogramowania jest równoważna w stosunku do oprogramowania opisanego przez Zamawiającego w niniejszym dokumencie, a także zgodnie z art. 30 ust. 5 Ustawy PZP wykazać, że rozwiązanie równoważne spełnia wymogi funkcjonalne, w tym w szczególności poprzez przedstawienie szczegółowego zestawienia i porównania funkcjonalności.

## Minimalne parametry równoważności dla oprogramowania do tworzenia kopii zapasowych

|  |  |
| --- | --- |
| **Wymagania ogólne** | • Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.0, 5.1, 5.5, 6.0, 6.5 oraz 6.7 oraz Microsoft Hyper-V 2012, 2012 R2, 2016 oraz 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej. |
|  | • Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. |
|  | • Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. |
|  | Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V |
| **Całkowite koszty posiadania** | • Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej |
|  | • Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków |
|  | • Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji |
|  | • Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli. |
|  | • Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. |
|  | • Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. |
|  | • Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania |
|  | • Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia |
|  | • Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie |
|  | • Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. |
|  | • Oprogramowanie musi oferować portal samoobłsugowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time) |
|  | • Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director 8.x i 9.x i archiwizować metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD. |
|  | • Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji |
|  | • Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji |
|  | • Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza |
|  | • Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) |
|  | • Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. |
| **Wymagania RPO** | • Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej |
|  | • Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych |
|  | • Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora |
|  | • Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn |
|  | • Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server |
|  | • Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej |
|  | • Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) |
|  | • Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC. |
|  | • Oprogramowanie musi umieć korzystać z protokołu Catalyst w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. |
|  | • Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. |
|  | • Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. |
|  | • Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik |
|  | • Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) |
|  | • Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V |
|  | • Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |
|  | • Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere |
|  | • Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing) |
| **Wymagania RTO** | • Oprogramowanie musi umożliwiać uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. Dla srodowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania |
|  | • Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami |
|  | • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków |
|  | • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2 |
|  | • Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików |
|  | • Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V |
|  | • Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: |
|  | o Linux |
|  | - ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs |
|  | o BSD |
|  | - UFS, UFS2 |
|  | o Solaris |
|  | - ZFS, UFS |
|  | o Mac |
|  | - HFS, HFS+ |
|  | o Windows |
|  | - NTFS, FAT, FAT32, ReFS |
|  | o Novell OES |
|  | - NSS |
|  | • Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces |
|  | • Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej |
|  | • Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites. |
|  | • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"), |
|  | • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat |
|  | • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień. |
|  | • Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. |
|  | • Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia. |
|  | • Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych. |
|  | • Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows |
|  | • Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |
| **Ograniczenie ryzyka** | • Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. |
|  | • Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem |
|  | • Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere |
|  | • Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. |
|  | • Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |
| **Monitoring** | • System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich |
|  | • System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.x oraz 6.x – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie |
|  | • System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. |
|  | • System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware |
|  | • System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter |
|  | • System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn |
|  | • System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel |
|  | • System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk |
|  | • System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora |
|  | • System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów |
|  | • System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) |
|  | • System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna |
|  | • System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego |
|  | • System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta |
|  | • System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. |
|  | • System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. |
|  | • System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware |
|  | • System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 8.x i 9.x |

# Prace konfiguracyjne i wdrożeniowe

Zamawiający oczekuje wykonania następujących czynności konfiguracyjnych i wdrożeniowych dla urządzeń i oprogramowania z punktów: **1, 2 i 6**:

1. Montaż urządzeń we wskazanych szafach rack 19’’.
2. Podłączenie do sieci zasilającej i wewnętrznej sieci LAN.
3. Uruchomienie urządzeń, sprawdzenie poprawności działania.
4. Instalacja i konfiguracja systemu operacyjnego (urządzenie 1).
5. Konfiguracja pracy w klastrze (urządzenie 1).
6. Przeprowadzenie testów funkcjonalnych działania uruchomionego klastra (urządzenie 1)
7. Konfiguracja adresacji IP (urządzenie 1).
8. Migrację obecnej konfiguracji i instancji maszyn wirtualnych do nowego systemu z uwzględnieniem optymalizacji ustawień uwzględniającej specyfikację techniczną nowo zakupionego urządzenia (urządzenie 1)
9. Sporządzenie dokumentacji powdrożeniowej zawierającej wykaz wykonanych prac i ustawionych parametrów pracy urządzeń oraz uwzględniającej architekturę, opis, schematy konfiguracji wdrożonych rozwiązań.
10. Uruchomienie produkcyjne.
11. Instalacja na nowo kupowanych przez Zamawiającego serwerach z pozycji 1 (pozycja 6).
12. Konfigurację podstawowych planów i harmonogramu tworzenia kopii (pozycja 6).
13. Przeprowadzenie testów funkcjonalnych w zakresie odtworzenia (pozycja 6).

Prace wdrożeniowe i konfiguracyjne odbywać się będą w dniach roboczych w godzinach:   
08:00 – 15:00

Do współpracy Wykonawcy Zamawiający wyznaczy przynajmniej jedną osobę, która będzie do dyspozycji w godzinach: 08:00-15:00

Konfiguracja i wdrożenie zostaną wykonane w uzgodnionym z Zamawiającym terminie, nie później jednak niż 2 miesiące od momentu dostarczenia do Zamawiającego urządzeń (urządzenia 1 i 2 oraz oprogramowanie z pozycji 6).

W okresie 3 miesięcy od daty podpisania protokołu odbioru końcowego Wykonawca zobowiązany będzie udzielać powdrożeniowej asysty technicznej i wsparcia drogą telefoniczną w trybie 8 godzin roboczych (7.30 -15.30) przez 5 dniu w tygodniu, w przypadku wystąpienia problemów lub wątpliwości, związanych z wykonaną dostawą i wdrożeniem w kwestiach związanych z:

a) konfiguracją

b) administrowaniem

c) analizą logów

Wsparcie powdrożeniowe w szczególnych przypadkach powinno obejmować wykonanie zdalnych prac przez pracownika Wykonawcy w ramach przedstawienia sposobu na rozwiązanie zaistniałych problemów.

# Wdrożenie dedykowanego narzędzia do analizy logów, zapisywania zdarzeń i raportowania

Zamawiający jest w posiadaniu narzędzia FortiAnalyzer FAZ-VM-BASE.

Przedmiotem niniejszego zadania jest jego instalacja, wdrożenie i przeszkolenie administracyjne w siedzibie Zamawiającego i na jego zasobach.

Aktywa Zamawiającego, pozostające w bezpośrednim lub pośrednim związku z przedmiotem zamówienia:

* UTM – 2 szt.
* switche – 4 szt.

W ramach wykonania usługi wdrożeniowej Wykonawca zobowiązany jest do:

1. Instalacji i konfiguracja narzędzia FortiAnalyzer we wskazanej przez Zamawiającego lokalizacji w siedzibie Zamawiającego,
2. Konfiguracja i podłączenie do narzędzia FortiAnalyzer urządzeń wskazanych przez Zamawiającego, w ilości nie mniejszej niż 6 szt.,
3. Konfiguracja automatyzacji zbierania i przechowywania logów w narzędziu FortiAnalyzer,
4. Konfiguracja automatyzacji procesów blokowania zagrożeń,
5. Konfiguracja opcji powiadamiania o zdarzeniach na e-mail,
6. Konfiguracja raportów,
7. Testy,
8. Przeprowadzenia szkolenia administratorów z monitorowania i raportowania,
9. Przygotowanie i przekazanie dokumentacji powdrożeniowej, uwzględniającej architekturę, opis, schematy konfiguracji wdrożonego rozwiązania (w wersji papierowej – 2 egzemplarze oraz elektronicznej, w postaci edytowalnej).

Wdrożenie zostanie zrealizowane w uzgodnionym z Zamawiającym terminie, nie później jednak niż 2 miesiące od momentu podpisania umowy.

W okresie 3 miesięcy od daty podpisania protokołu odbioru końcowego Wykonawca zobowiązany będzie udzielać powdrożeniowej asysty technicznej i wsparcia drogą telefoniczną w trybie 8 godzin roboczych (7:30 -15:30) przez 5 dni w tygodniu w przypadku wystąpienia problemów lub wątpliwości związanych z wykonanym wdrożeniem w kwestiach związanych z:

1. konfiguracją
2. administrowaniem
3. analizą logów

Wsparcie powdrożeniowe w szczególnych przypadkach musi obejmować wykonanie zdalnych prac przez pracownika Wykonawcy w ramach przedstawienia sposobu na rozwiązanie zaistniałych problemów.

Dedykowane do wykonania usługi osoby muszą wykazać się imiennym certyfikatem producenta wdrażanego rozwiązania na poziomie NSE5 oraz NSE7.