Załącznik nr 3

Szczegółowy opis przedmiotu zamówienia części III

|  |  |
| --- | --- |
| **Przedmiot zamówienia:** | **Zasilacz awaryjny UPS** |
| **Ilość:** | 1 sztuka |
| **Okres gwarancji producenta:**  | 36 m-cy |
| **Parametry** |
| Obudowa  | Uniwersalna tower/rack max. 2U |
| Moc, napięcia, gniazda, ochrony, dodatkowe dane | Moc pozorna: 3000 VAMoc rzeczywista: 3000 WWspółczynnik mocy: 1Topologia (klasyfikacja IEC 62040-3): line-interactiveLiczba, typ gniazd wyjściowych: 8 x C13, 2 x C19Typ gniazda wejściowego: Gniazdo C20Czas podtrzymania dla 100% obciążenia: 3 minutyNapięcie znamionowe: 230 V Tolerancja napięcia prostownika: 160 - 294 V (regulowana do 150 - 294 V)Częstotliwość znamionowa: 50/60 Hz autodetekcjaTolerancja częstotliwości: 47 - 70 Hz (system 50 Hz); 56,5 - 70 Hz (system 60 Hz); 40 Hz w trybie niskiej czułościNapięcie znamionowe wyjściowe: 230 V (domyślnie) / 200/208/220/240 VCzęstotliwość wyjściowa: 50/60 HzBaterie wymieniane przez użytkownika "na gorąco": TakOchrona przed przeładowaniem: TakOchrona przed głębokim rozładowaniem: TakOkresowy automatyczny test baterii: TakZimny start: TakMax. wymiary UPS (szer. x gł. x wys. w mm): 438 x 603 x 85,5Poziom hałasu w odl. 1m: < 45 dBA |
| System zarządzania pracą baterii | System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony. |
| Interfejs komunikacyjny | USB, RS232 DB-9 żeński (HID), miniport wyłącznik awaryjny RPO, miniport wyłącznik ON/OFF, listwa zaciskowa dla przekaźnika wyjściowego |
| Panel sterowania z wyświetlaczem LCD | Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS’a) ze wskazaniami chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh) |
| Przyciski sterujące i wskaźniki diodowe LED | Poziomy rząd przycisków sterowania; Poziomy rząd wskaźników stanu: trybu normalnego (zielony), trybu bateryjnego (żółty), usterki (czerwony); Pasek LED sygnalizujący stan; sygnalizator akustyczny (awaria, serwis, niski stan naładowania baterii, przeciążenie); przycisk Escape (anulowanie); przyciski funkcyjne (przewijanie w górę i w dół); przycisk Enter (potwierdzający) |
| Wyposażenie | UPS 3 kVA, instrukcja obsługi, instrukcja bezpieczeństwa; przewód zasilający; kabel RS232; kabel USB; karta SNMP; uchwyty kablowe; podstawki do montażu pionowego (wieża); 2 przewody IEC 10 A; zestaw szyn montażowych do szafy 19" Karta SNMP "cyberbezpieczeństwo (certyfikaty UL 2900-2-2 /IEC62443 /HTTPS/MQTT/NDIS/LDAP/NVD//SSH/PKI, pakiet szyfrów TLS 1.2 z minimum SHA256)"; certyfikaty CA i PKl; prędkość gigabitowa (half-duplex, full-duplex); różne poziomy nadawania dostępu do konta administratora lub użytkownika |
| Dołączone oprogramowanie | Do bezpiecznego zamykania systemów operacyjnych przy wyczerpaniu baterii (minimum: Windows: 10, 2000, XP, 2003, Vista, Server 2008, 7; Linux: Red Hat, Fedora Core, SuSE; UNIX: AIX, HP-UX, SCO, SGI Irix, Mac OS, Sun Solaris; Novell NetWare do v 6.5). Oprogramowanie musi mieć możliwość wyboru polskiej wersji językowej. |
| Zgodność z normami UE | Deklaracja zgodności producenta |
| Dodatkowe cetyfikaty | ISO9001 producenta urządzenia |
|  |

|  |  |
| --- | --- |
| **Przedmiot zamówienia:** | **Usługi wdrożeniowe UPS** |
| **Opis przedmiotu zamówienia:** | Wdrożenie usługi zarządzania zasilaniem serwera działającego w oparciu o hypervisor ESXi VMware. Usługa obejmuje automatyczne wyłączanie i załączanie serwera poprzez komunikację z hypervisorem za pomocą karty sieciowej akredytowanej przez producenta wirtualizacji. |
| **Ilość:** | 1 sztuka |
| **Parametry** |
| Zakres prac wdrożeniowych | Analiza środowiska IT Zamawiającego: Przegląd i analiza aktualnej infrastruktury IT w celu dopasowania konfiguracji usługi zarządzania zasilaniem.Instalacja niezbędnego oprogramowania: instalacja wszystkich komponentów programowych w tym ich rejestracja i aktywacja na dane Zamawiającego.Konfiguracja hypervisora ESXi VMware: Dostosowanie ustawień hypervisora do współpracy z urządzeniem UPS, w tym skonfigurowanie protokołów komunikacyjnych i automatycznych procedur wyłączania oraz załączania serwera.Integracja z istniejącą infrastrukturą IT: Podłączenie urządzenia UPS do istniejącej infrastruktury sieciowej i zapewnienie pełnej integracji z systemami zarządzania IT.Automatyzacja procesów zarządzania zasilaniem: Konfiguracja procedur automatycznego wyłączania serwera w przypadku awarii zasilania oraz jego ponownego uruchamiania po przywróceniu zasilania, zgodnie z wymaganiami Zamawiającego.Testowanie i optymalizacja: Przeprowadzenie testów funkcjonalnych i obciążeniowych, aby upewnić się, że wszystkie procesy automatyzacji działają poprawnie. Optymalizacja konfiguracji na podstawie wyników testów.Miejsce wykonywania usług: Wszystkie prace muszą zostać wykonane w siedzibie zamawiającego. |
| Szkolenie i wsparcie dla IT | Szkolenie dla zespołu IT Zamawiającego: Przeprowadzenie szkoleń w zakresie obsługi i zarządzania nowo wdrożoną usługą zarządzania zasilaniem. Szkolenia obejmują procedury wyłączania i załączania serwera, zarządzanie alarmami oraz monitorowanie stanu zasilania. Szkolenia muszą zostać wykonane na środowisku IT w siedzibie Zamawiającego.Dokumentacja techniczna: Dostarczenie szczegółowej dokumentacji opisującej wszystkie przeprowadzone konfiguracje, procedury zarządzania oraz instrukcje obsługi. |
| Wsparcie i serwis | Wsparcie techniczne: Zapewnienie wsparcia technicznego przez okres 24 miesięcy od daty zakończenia wdrożenia. W przypadku awarii, wykonawca zapewni naprawę zdalną w czasie do 5 godzin, a w razie konieczności, fizyczną naprawę na miejscu w ciągu 24 godzin.Kontakt: Wykonawca udostępni kontakt e-mail i telefoniczny do zgłaszania awarii i problemów technicznych. Czas reakcji liczony od momentu wysłania zgłoszenia przez Zamawiającego. |
| Zgodność z normami i przepisami | Wykonanie usługi zgodnie z Polską Normą PN-ISO/IEC 27002.Zgodność z Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności określającym minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalne wymagania dla systemów teleinformatycznych. |
| Zakończenie prac | Prace wdrożeniowe zostaną zakończone protokołem odbioru, który będzie zawierał wszystkie wykonane prace oraz konfiguracje. |

|  |  |
| --- | --- |
| **Przedmiot zamówienia:** | **UTM wraz ze wsparciem oraz licencją na 2 lata** |
| **Ilość:** | 1 sztuka |
| **Okres gwarancji producenta:**  | 24 m-ce |
| **Parametry** |
| Wymagania Ogólne | System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.System wspiera protokoły 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 – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych
 |
| Interfejsy, Dysk, Zasilanie: | 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
	1. 10 portami Gigabit Ethernet RJ-45.
	2. 2 gniazdami SFP 1 Gbps.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System jest wyposażony w zasilanie AC.
 |
| Funkcje Systemu Bezpieczeństwa: | W ramach systemu ochrony są 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.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są 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. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
 |
| Polityki, Firewall | 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
	1. Translację jeden do jeden oraz jeden do wielu.
	2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
	1. Amazon Web Services (AWS).
	2. Microsoft Azure.
	3. Cisco ACI.Google Cloud Platform (GCP).
	4. OpenStack.
	5. VMware NSX.
	6. Kubernetes.
 |
| Połączenia VPN | 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
	1. Wsparcie dla IKE v1 oraz v2.
	2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
	3. Obsługa protokołu Diffie-Hellman grup 19, 20.
	4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
	5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
	6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
	7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
	8. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
	9. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
	10. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
	11. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
	12. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
	1. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
	2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
	3. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
 |
| Routing i obsługa łączy WAN | W zakresie routingu rozwiązanie zapewnia obsługę:1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
 |
| Funkcje SD-WAN | 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
 |
| Zarządzanie pasmem | 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
 |
| Ochrona przed malware | 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
 |
| Ochrona przed atakami | 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System zapewnia 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).
6. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
 |
| Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
6. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
 |
| Kontrola WWW | 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
 |
| Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall umożliwia 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.
1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
 |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
 |
| Logowanie | 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
 |
| Serwisy i licencje | Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy. |
| Gwarancja oraz wsparcie | System musi być objęty serwisem gwarancyjnym producenta przez okres 24 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. |
|  |

|  |  |
| --- | --- |
| **Przedmiot zamówienia:** | **Switch POE z licencjami na 2 lata** |
| **Ilość:** | 1 sztuka |
| **Okres gwarancji producenta:**  | 24 m-ce |
| **Parametry** |
| Przełącznik sieciowy | W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. |
| Parametry fizyczne platformy | * Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
* Zasilanie AC 230V.
 |
| Interfejsy sieciowe | Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:* 24 porty GE RJ-45, w tym porty PoE w ilości co najmniej: 12, zgodne ze standardem: 802.3af/at.
* 4 porty 10 GE SFP+.
 |
| Zarządzanie | * Wbudowany port konsoli szeregowej do pełnego zarządzania.
* Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
* 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 z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
* Automatycznie wykonywane rewizje konfiguracji.
 |
| 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 VLAN'ów, zgodna ze standardem 802.1Q.
* Port-mirroring.
* Uwierzytelnianie 802.1x na poziomie portu.
* Uwierzytelnianie 802.1x w oparciu o adres MAC.
* W ramach 802.1x wsparcie dla dedykowanego VLAN'u 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.
 |
| 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:
	* Centralne zarządzanie konfiguracją urządzenia
	* Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
	* Centralne zarządzanie sieciami VLAN.
	* Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
	* Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
	* Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
	* Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
	* Automatyczna detekcja i rekomendacje konfiguracji.
	* Przesyłanie logów na zewnętrzny serwer syslog.
	* Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
	* Obsługa białych i czarnych list adresów MAC.
	* Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
 |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa | * System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym
* System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
 |
| Gwarancja oraz wsparcie | System musi być objęty serwisem gwarancyjnym producenta przez okres 24 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. |
|  |

|  |  |
| --- | --- |
| **Przedmiot zamówienia:** | **Switch z licencjami na 2 lata** |
| **Ilość:** | 2 sztuki |
| **Okres gwarancji producenta:**  | 24 m-ce |
| **Parametry** |
| Przełącznik sieciowy | W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. |
| Parametry fizyczne platformy | * Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
* Zasilanie AC 230V.
 |
| Interfejsy sieciowe - wymagania minimalne | 1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
	1. 48 porty GE RJ-45.
	2. 4 porty 10 GE SFP+.
 |
| Zarządzanie | * 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 z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
* Automatycznie wykonywane rewizje konfiguracji.
 |
| 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 VLAN'ów, zgodna ze standardem 802.1Q.
* Port-mirroring.
* Uwierzytelnianie 802.1x na poziomie portu.
* Uwierzytelnianie 802.1x w oparciu o adres MAC.
* W ramach 802.1x wsparcie dla dedykowanego VLAN'u 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.
 |
| 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:
	* Centralne zarządzanie konfiguracją urządzenia
	* Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
	* Centralne zarządzanie sieciami VLAN.
	* Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
	* Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
	* Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
	* Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
	* Automatyczna detekcja i rekomendacje konfiguracji.
	* Przesyłanie logów na zewnętrzny serwer syslog.
	* Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
	* Obsługa białych i czarnych list adresów MAC.
	* Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
 |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa | * System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
* System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
 |
| Gwarancja oraz wsparcie | System musi być objęty serwisem gwarancyjnym producenta przez okres 24 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. |
|  |

|  |  |
| --- | --- |
| **Przedmiot zamówienia:** | **Punkt dostępowy sieci bezprzewodowej z licencjami na 2 lata** |
| **Ilość:** | 3 sztuki |
| **Okres gwarancji producenta:**  | 24 m-ce |
| **Parametry** |
| Opis | Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. |
| Dane techniczne | 1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
	1. Temperatura 0–50°C,
	2. Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington.
3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
	1. 2.4 GHz lub 5.0 GHz a/b/g/n/ac/ax,
	2. 5.0 GHz a/n/ac/ax,
	3. 2.4 GHz service b/g/n/ax
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.
5. Urządzenie musi być wyposażone w moduł BLE/ZigBee.
6. Urządzenie musi być wyposażone w dwa interfejsy Ethernet 10/100/1000 Base-TX oraz interfejs konfiguracyjny RS-232 RJ45.
7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz.
8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
	1. Tunnel,
	2. Bridge,
	3. Mesh.
9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
	1. MIMO – 2x2,
	2. Maksymalna przepustowość dla poszczególnych modułów radiowych:
		1. 1201 Mbps;
		2. 1201 Mbps;
		3. 574 Mbps.
	3. Wymagana moc nadawania:
		1. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
		2. min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
	4. Wsparcie dla 802.11n 20/40Mhz HT,
	5. Wsparcie dla kanałów 80MHz,
	6. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 3.5dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.
	7. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
	8. Maksymalna deklarowana liczba klientów per moduł radiowy:
		1. 512;
		2. 512;
		3. 512.
12. Funkcje dodatkowe:
	1. OFDMA
	2. Spatial Reuse (BSS Coloring)
	3. UL-MU-MIMO 802.11ax
	4. DL-MU-MIMO
	5. Enhanced Target Wake Time (TWT)
 |
| Gwarancja oraz wsparcie | Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 24 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. |
|  |

|  |  |
| --- | --- |
| **Przedmiot zamówienia:** | **Usługi wdrożeniowe** |
| **Opis przedmiotu zamówienia:** | Wdrożenie urządzenia UTM oraz pozostałych urządzeń sieciowych tego samego producenta wraz z wszystkimi czynnościami i procedurami nakazanymi przez producenta i wymogi prawa pozwalającymi używać ich w sposób zgodny i bezpieczny do przetwarzania informacji. |
| **Ilość:** | 1 sztuka |
| **Parametry** |
| Uszczegółowienie | Wdrożenie UTM, przełączników sieciowych klasy enterprise i urządzeń sieci bezprzewodowych tego tergo samego producenta. Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencję), przypisanie licencji do emaila wskazanego przez Zamawiającego.Aktualizacja do najmowych wersji oprogramowania.Wydzielenie podsieci VLAN w tym sieci bezprzewodowych zgodnie z wskazaniami Zamawiającego. Zabezpieczenie ruchu we wszystkich podsieciach zgonie w wymaganiami Zamawiającego.Integracja z Istniejącym środowiskiem IT.Wdrożenie VPN – konfiguracja, integracja z GPO i zabezpieczenie Tuneli VPN. Wdrożenie wydzielonej – galwanicznej sieci zarządzającej systemami IT.Wdrożenie wykonywane na miejscu.Dwuletnie nieodpłatne wsparcie ze trony pracowników Wykonawcy w w/w zakresie.Przez 24 miesiące od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych - Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu.Wykonawca udostępni kontakt email i telefoniczny. Czas jest liczony od wysłania e-mail przez Zamawiającego. |
| Zgodność z normami i przepisami | Polską Normą PN-ISO/IEC 27002,Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych. |
| Zakończenie prac | Prace zostaną zakończone protokołem. |

|  |  |
| --- | --- |
| **Przedmiot zamówienia:** | **Pamięci RAM dedykowane do serwera posiadanego przez zamawiającego Dell PowerEdge R540 o numerze seryjnym 9XFF6R3** |
| **Ilość:** | 2 sztuki |
| **Okres gwarancji producenta:**  | Objęte gwarancją serwera posiadanego przez zamawiającego – Dell PowerEdge R540 o numerze seryjnym 9XFF6R3 |
| **Parametry** |
| Opis | Pamięci o pojemności 64GB dedykowane do serwera posiadanego przez zamawiającego: Dell PowerEdge R540 o numerze seryjnym 9XFF6R3 |
|  |

|  |  |
| --- | --- |
| **Przedmiot zamówienia:** | **Usługi wdrożeniowe**  |
| **Ilość:** | 1 sztuka |
| **Parametry** |
| Wdrożenie iDRAC wraz ze wsparciem | Wdrożenie zintegrowanego modułu zdalnego zarządzania serwerem.Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencję), przypisanie licencji do emaila wskazanego przez Zamawiającego.Aktualizacja do najnowszej wersji oprogramowania.Zapewnienie konfiguracji wszystkich parametrów w tym macierzy dyskowych zgodnie z wymogami prawa i wytycznymi Zamawiającego.Podłączenie do podsieci zgodnie w wymaganiami Zamawiającego. Integracja z istniejącym środowiskiem IT.Dwuletnie nieodpłatne wsparcie ze trony pracowników Wykonawcy w w/w zakresie.Przez 24 miesiące od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych - Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu.Wykonawca udostępni kontakt email i telefoniczny. Czas jest liczony od wysłania e-mail przez Zamawiającego. |
| Instalacja Hypevisora | Fizyczna i techniczna Instalacja oprogramowania ESXi w siedzibie Zamawiającego wraz z pełną konfiguracją. Migracja starego środowiska na nowy Hypervisor. Migracja musi odbyć się z rozbiciem na poszczególne serwery wirtualne zgodnie z wskazaniami Zamawiającego. Proces przejścia z starego na nowy serwer trzeba wykonać po godzina pracy instytucji - aby zachować ciągłość pracy Zamawiającego.Wdrożenie wykonywane w siedzibie Zamawiającego. |
| Konfiguracja macierzy dyskowych | Konfiguracja macierzy dyskowej na serwerze zamawiającego, instalacja aktualnego firmware, konfiguracja RAID z dyskiem hot-spare. |
| Separacja sieci roboczych od zarządzających | Wdrożenie wydzielonej, galwanicznej sieci wirtualnej, zarządzającej systemami IT do wykonywania kopii serwera wirtualnego.Wdrożenie sieci wirtualnych i integracja z UTM zamawiającego. |
| Dostosowanie konfiguracji hypervisor do wymogów KRI | Dostosowanie konfiguracji do wymogów KRI zgodnie z* § 20 ust.2. pkt 1 KRI (t.j. Dz.U. z 2024, poz. 773)
* § 20 ust.3. pkt 1 KRI (t.j. Dz.U. z 2024, poz. 773)
* § 20 ust.3. pkt 2 KRI (t.j. Dz.U. z 2024, poz. 773)
* § 20 ust.3. pkt 3 KRI (t.j. Dz.U. z 2024, poz. 773)

Uniemożliwienie nieautoryzowanego dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji zgodnie z § 19 ust.2. pkt 7 lit.c KRI (t.j. Dz.U. z 2024, poz. 773) PN-ISO/IEC 27002 ust.9.1.2 |
| Przygotowanie serwera kopii bezpieczeństwa wraz systemem operacyjnym | Instalacja systemu operacyjnego oraz konfiguracja serwera kopii bezpieczeństwa. |
| Instalacja programu wraz z bazą danych | Instalacja bazy danych. Instalacja oprogramowania do wykonywania kopii bezpieczeństwa wykorzystującego technologię deduplikacji maszyn wirtualnych oraz konfiguracja oprogramowania wraz z bazą danych. |
| Przygotowanie repozytorium lokalnego | Przygotowanie repozytorium lokalnego na serwerze kopii bezpieczeństwa. |
| Przygotowanie dodatkowego repozytorium opartego o serwer NAS w siedzibie organizacji | Przygotowanie repozytorium dodatkowego na serwerze NAS zamawiającego. |
| Podłączenie do zdalnego repozytorium z konfiguracją VPN | Wdrożenie połączenia z wykorzystaniem technologii VLAN w sieci lokalnej oraz VPN pomiędzy serwerem kopii zapasowej a repozytorium zdalnym mieszczącym się na serwerze NAS zamawiającego. |
| Instalacja kontrolera domeny Windows Server | Instalacja maszyn wirtualnych, systemów operacyjnych i przygotowanie serwerów w tym kontrolerów domeny na potrzeby pracy w Domenie Systemu Windows.Migracja istniejącego środowiska IT Zamawiającego. W przypadku braku możliwości migracji istniejących rozwiązań, wdrożenie od podstaw nowej domeny wraz z przeniesieniem zasobów.Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencję), przypisanie licencji do emaila wskazanego przez Zamawiającego.Aktualizacja do najmowych wersji oprogramowania.Wdrożenie i zabezpieczenie usługi DNS.Przygotowanie maszyn wirtualnych na potrzeby baz danych, podłączenie do domeny oraz ich zabezpieczenie.Dwuletnie nieodpłatne wsparcie ze trony pracowników Wykonawcy w ww. zakresie.Przez 24 miesiące od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych - Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu.Wykonawca udostępni kontakt email i telefoniczny. Czas jest liczony od wysłania e-mail przez Zamawiającego.Udzielenie zdalnego wsparcia dla pracowników IT Zamawiającego, nie będącego następstwem błędów i awarii w liczbie 30 godzin.Prace zostaną zakończone protokołem |
| Wdrożenie polis GPO dostosowujących środowisko do wymogów rozporządzenia KRI | Wdrożenie polis GPO dostosowujących środowisko do ww. wymogów prawa i Zamawiającego - takich jak polisy synchronizacji czasu, dokumentów, haseł, blokowania, dostępu do zasobów, etc. |
| Wdrożenie serwera plików AD | Wdrożenie usługi File Server, utworzenie, przeniesienie, przypisanie uprawnień i zabezpieczenie zasobów zgodnie z zaleceniami Zamawiającego. (np. dyski wspólne z podziałem uprawnień) |
| Wdrożenie serwera wydruków AD | Wdrożenie usługi Print Server, wraz z konfiguracją i zabezpieczeniami. |
| Migracja i zabezpiecznie baz SQL | Migracja baz danych opartych o technologię SQL w środowisku zamawiającego do wdrażanego środowiska opartego o technologię wirtualizacji działającego w usłudze katalogowej AD.  |
| Wsparcia dla osoby przenoszącej systemy w liczbie 10 godzin | Wsparcie lokalne lub zdalne dla osoby delegowanej przez Zamawiającego przenoszącej systemy w liczbie nie więcej niż 10 godzin. |
| Wsparcia dla osoby przenoszącej profile użytkowników Windows do środowiska AD w liczbie 10 godzin | Wsparcie lokalne lub zdalne dla osoby delegowanej przez Zamawiającego przenoszącej profile użytkowników Windows do środowiska usługi katalogowej AD w liczbie nie więcej niż 10 godzin. |
| Wdrożenie agenta ESET w oparciu o mechanizm dystrybucji usługi katalogowej Active Directory | Instalacja maszyny wirtualnej, systemów operacyjnych i przygotowanie systemu antywirusowego.Wdrożenie polis GPO umożliwiających dystrybucję spreparowanego agenta w sieci zamawiającego.Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencję), przypisanie licencji do emaila wskazanego przez Zamawiającego.Aktualizacja do najnowszych wersji oprogramowania.Wykonanie konfiguracji (np. blokowanie nośników) zgodnie z wskazaniami Zamawiającego.Dwuletnie nieodpłatne wsparcie ze trony pracowników Wykonawcy w ww. zakresie.Przez 24 miesiące od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych - Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu.Wykonawca udostępni kontakt email i telefoniczny. Czas jest liczony od wysłania e-mail przez Zamawiającego.Prace zostaną zakończone protokołem. |
| Zgodność | Usługi muszą zawierać wymagane konfiguracje i zostać wykonane zgodnie z:* Polską Normą PN-ISO/IEC 27002,
* Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
 |
|  |

|  |  |
| --- | --- |
| **Przedmiot zamówienia:** | **Agregacja logów** |
| **Ilość:** | 1 sztuka |
| **Okres gwarancji producenta:**  | 24 m-ce |
| **Parametry** |
| Opis | Przedmiot zamówienia stanowi świadczenie usług przechowywania logów systemowych pochodzących z Kontrolera Domeny i urządzenia UTM Zamawiającego, z wykorzystaniem bezpiecznego połączenia VPN. Usługa ta ma na celu zapewnienie bezpieczeństwa oraz możliwości rozliczenia działań zgodnie z obowiązującymi wymogami prawnymi. |
| Zakres usługi | Konfiguracja i zarządzanie połączeniem VPN, umożliwiające przesyłanie logów z systemów Zamawiającego do systemów IT przechowujące dane u Wykonawcy. Połączenie musi spełniać następujące kryteria:* Komunikacja sieciowa możliwa tylko w kierunku od Zamawiającego do Wykonawcy.
* Zapobieganie inicjowaniu połączenia od Wykonawcy do Zamawiającego.
* Wykluczenie możliwości routowania z VPN do wewnętrznych sieci komputerowych Zamawiającego.
 |
| Zarejestrowane logi muszą zawierać szczegółowe informacje dotyczące:* dostępu użytkowników do systemów lub zbiorów danych,
* zmian w konfiguracji zabezpieczeń,
* dostępu do informacji objętych ochroną prawną, zdarzeń systemowych.
 |
| Przechowywanie logów przez okres co najmniej 24 miesięcy, nawet po zakończeniu świadczenia usługi. Wykonawca musi zapewnić przechowywanie wcześniej zebranych logów przez 24 miesiące od ich zebrania niezależnie od zaprzestania świadczenia usługi. Zamawiający może zażądać usunięcia zebranych logów poprzez przekazanie dokumentu podpisanego przez osobę uprawnioną. |
| Wykonawca dostarcza rozwiązania techniczne gwarantujące, zabezpieczenie logów przed edycją i nieautoryzowanym usunięciem. |
| Zgodność | Usługa musi być zgodna z:* Polską Normą PN-ISO/IEC 27002,
* Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych
 |
|  |

|  |  |
| --- | --- |
| **Przedmiot zamówienia:** | **Szkolenia IT wraz ze wsparciem** |
| **Ilość:** | 1 sztuka |
| **Parametry** |
| Opis | Zakres szkoleń:* Szkolenie dla IT - Szkolenie z obsługi systemu Windows Server 2022, usługi katalogowej Active Directory, funkcji Print Server oraz zasad grupy GPO;
* Szkolenie dla IT - Szkolenie z obsługi oprogramowania Veeam;
* Szkolenie dla IT - Szkolenie z zastosowanych rozwiązań UTM.

Wszystkie szkolenia wykonane w siedzibie zamawiającego. Szkolenia należy wykonać z uwzględnieniem konfiguracji zastosowanych w systemach IT Zamawiającego. Wykonawca musi posiadać status partnera wszystkich producentów zastosowanych rozwiązań. Osoby prowadzące szkolenia muszą posiadać udokumentowaną wiedzę. Szkolenia zakończone protokołem.Wykonawca zapewni nieodpłatne wsparcie w ww. zakresie przez okres 24 miesięcy od zakończenia szkolenia w liczbie 30 godzin. Wsparcie zostanie udzielone w terminie 48 godzin od chwili zgłoszenia.Wykonawca udostępni kontakt email i telefoniczny. Czas jest liczony od wysłania e-mail przez Zamawiającego.Prace zostaną zakończone protokołem. |
|  |