Załącznik nr 2 do SWZ

**Specyfikacja techniczna**

# **1. Dostawa, montaż i konfiguracja trzech sztuk urządzeń bezpieczeństwa sieci dla Urzędu Gminy Ożarowice, Ośrodka Pomocy Społecznej, Zakładu Gospodarki Komunalnej**

## **1.1 Urządzenie bezpieczeństwa sieci - 1 szt. (dla Urzędu Gminy Ożarowice)**

**Marka: …………………………..**

**Model: …………………………..**

|  |  |  |
| --- | --- | --- |
| **Minimalne wymagania** | | **Parametr oferowany** |
| **System** | | |
| **Konstrukcja** | | |
| System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania. | | Tak/Nie |
| Rozwiązanie powinno być wyposażone w moduł kryptoraficzny zgodny ze standardem FIPS 140-2. | | Tak/Nie |
| Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca) | | Tak/Nie |
| Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie Active-Passive lub Active-Active. | | Tak/Nie |
| System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej. | | Tak/Nie |
| Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy. | | Tak/Nie |
| Urządzenie w metalowej obudowie z możliwością montażu w szafie rack 19". | | Tak/Nie |
| Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB). | | Tak/Nie |
| Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie. | | Tak/Nie |
| Wbudowany port USB umożliwiający podłączenie pamięci flash i przeprowadzenie konfiguracji w trybie Zero Touch. | | Tak/Nie |
| Możliwość rozbudowy o dodatkowe moduły interfejsów sieciowych. | | Tak/Nie |
| Pamięć operacyjna RAM nie mniej niż (GB): | 8 | Tak/Nie |
| Przestrzeń do przechowywania logów i raportów nie mniej niż (GB) | 64 | Tak/Nie |
| Liczba fizycznych interfejsów 1000BASE-T nie mniej niż: | 6 | Tak/Nie |
| Liczba fizycznych interfejsów 1000BASE-X nie mniej niż: | 2 | Tak/Nie |
| Liczba fizycznych interfejsów 1000BASE-T ze wsparciem PoE 30W nie mniej niż: | 2 | Tak/Nie |
| Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q nie mniej niż: | 128 | Tak/Nie |
| **Wydajność** | | |
| Wydajność Firewall nie mniej niż (Mbps) | 19 000 | Tak/Nie |
| Wydajność Firewall IMIX nie mniej niż (Mbps) | 10 500 | Tak/Nie |
| Wydajność IPS nie mniej niż (Mbps) | 5 500 | Tak/Nie |
| Wydajność FW+IPS+AV nie mniej niż (Mbps) | 4 500 | Tak/Nie |
| Wydajność NGFW nie mniej niż (Mbps) | 5 000 | Tak/Nie |
| Liczba równoczesnych połączeń nie mniejsza niż: | 6 500 000 | Tak/Nie |
| Liczba nowych połączeń na sekundę nie mniejsza niż: | 100 000 | Tak/Nie |
| Wydajność IPsec VPN nie mniej niż (Mbps): | 6 500 | Tak/Nie |
| Liczba równoczesnych tuneli IPsec VPN nie mniejsza niż: | 2 500 | Tak/Nie |
| Liczba równoczesnych tuneli SSL VPN nie mniejsza niż: | 1 500 | Tak/Nie |
| Wydajność dla inspekcji ruchu SSL/TLS nie mniej niż (Mbps): | 1 500 | Tak/Nie |
| Liczba równoczesnych połączeń SSL/TLS nie mniejsza niż: | 18 000 | Tak/Nie |
| **Zarządzanie** | | |
| Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. | | Tak/Nie |
| Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). | | Tak/Nie |
| Rozwiązanie powinno oferować wsparcie dla generowania certyfikatów za pomocą firmy Let’s Encrypt. | | Tak/Nie |
| Rozwiązanie powinno oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. | | Tak/Nie |
| Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter. | | Tak/Nie |
| Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. | | Tak/Nie |
| Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. | | Tak/Nie |
| System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. | | Tak/Nie |
| System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. | | Tak/Nie |
| System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. | | Tak/Nie |
| Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). | | Tak/Nie |
| System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. | | Tak/Nie |
| Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). | | Tak/Nie |
| System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog). | | Tak/Nie |
| Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej. | | Tak/Nie |
| System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS). | | Tak/Nie |
| Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta. | | Tak/Nie |
| System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpowiednik). | | Tak/Nie |
| System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia. | | Tak/Nie |
| System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta. | | Tak/Nie |
| Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji z zapisem do pliku na komputer administratora, na serwer FTP, lub na email. | | Tak/Nie |
| Rozwiązanie powinno oferować wbudowany mechanizm pozwalający na automatyczne tworzenie szyfrowanych hasłem kopii zapasowych konfiguracji w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu. | | Tak/Nie |
| Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich. | | Tak/Nie |
| Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). Informacja o dostępności nowej wersji powinna pojawiać się w Web GUI. | | Tak/Nie |
| Producent powinien oferować mechanizm automatycznego łatania wykrytych w oprogramowaniu systemowym podatności przez tzw. hotfixies, przy czym administrator powinien móc funkcjonalność tą wyłączyć. | | Tak/Nie |
| **Zapora sieciowa, konfiguracja sieciowa oraz routing** | | |
| **Zapora sieciowa** | | |
| Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection. | | Tak/Nie |
| System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas. | | Tak/Nie |
| System powinien pozwalać na selektywne wyłączanie reguł zapory sieciowej (bez konieczności ich usuwania). | | Tak/Nie |
| System powinien pozwalać na grupowanie reguł zapory. Wymagana jest funkcjonalność automatycznego wiązania nowotworzonych reguł do właściwych grup na podstawie kryteriów opisujących grupę. | | Tak/Nie |
| Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. | | Tak/Nie |
| System ochrony powinien zawierać predefiniowane strefy zapory typu: LAN, WAN, DMZ, VPN. | | Tak/Nie |
| Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej. | | Tak/Nie |
| System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). | | Tak/Nie |
| Rozwiązanie powinno oferować narzędzie do symulowanego testu reguł zapory w oparciu o zadane przez administratora kryteria takie jak IP, strefa zapory, użytkownik, dzień, godzina. | | Tak/Nie |
| **Trasowanie ruchu** | | |
| Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing. | | Tak/Nie |
| Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. | | Tak/Nie |
| Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać rozkładanie ruchu w oparciu o wagi interfejsów WAN. | | Tak/Nie |
| Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast. | | Tak/Nie |
| Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). | | Tak/Nie |
| Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM). | | Tak/Nie |
| Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6. | | Tak/Nie |
| **Translacja adresów i portów** | | |
| Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT. | | Tak/Nie |
| Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT. | | Tak/Nie |
| Rozwiązanie powinno pozwalać na automatyczne tworzenie reguł NAT typu loopback czy reflexive rule. | | Tak/Nie |
| **Kształtowanie pasma i jakość usług** | | |
| System powinien zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji. | | Tak/Nie |
| Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne. | | Tak/Nie |
| System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. | | Tak/Nie |
| Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6. | | Tak/Nie |
| Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet. | | Tak/Nie |
| **Podstawowa ochrona przed atakami DoS i DDoS** | | |
| System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection). | | Tak/Nie |
| **Pozostałe** | | |
| Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. | | Tak/Nie |
| Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge). | | Tak/Nie |
| System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. | | Tak/Nie |
| System powinien oferować wsparcie dla IEEE 802.3Q VLAN z możliwością konfiguracji niezależnych puli DHCP. | | Tak/Nie |
| Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). | | Tak/Nie |
| System powinien oferować wsparcie dla usług Dynamic DNS takich jak np. DynDNS, ZoneEdit, EasyDNS, DynAcces itp. | | Tak/Nie |
| Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd). | | Tak/Nie |
| Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo). | | Tak/Nie |
| Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych. | | Tak/Nie |
| **Uwierzytelnianie i obsługa użytkowników** | | |
| Wymagane uwierzytelnianie użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta. | | Tak/Nie |
| Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników. | | Tak/Nie |
| System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory. | | Tak/Nie |
| System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm). | | Tak/Nie |
| Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server. | | Tak/Nie |
| System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. | | Tak/Nie |
| Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu. | | Tak/Nie |
| **Koncentrator VPN** | | |
| System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2. | | Tak/Nie |
| System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519). | | Tak/Nie |
| System musi obsługiwać połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN. | | Tak/Nie |
| Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN. | | Tak/Nie |
| Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback. | | Tak/Nie |
| Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego. | | Tak/Nie |
| Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth. | | Tak/Nie |
| Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połaczeń IPsec client-to-site VPN jak i SSL client-to-site VPN. | | Tak/Nie |
| Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN. | | Tak/Nie |
| Urządzenie musi obsługiwać połączenia L2TP over IPsec. | | Tak/Nie |
| **Logowanie i raportowanie** | | |
| System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym. | | Tak/Nie |
| System powinien umożliwiać składowanie oraz archiwizację logów. | | Tak/Nie |
| Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. | | Tak/Nie |
| Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów. | | Tak/Nie |
| Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa. | | Tak/Nie |
| System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali. | | Tak/Nie |
| System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać wysyłanie raportów via email. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV. | | Tak/Nie |
| Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog. | | Tak/Nie |
| System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza. | | Tak/Nie |
| System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację. | | Tak/Nie |
| Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach. | | Tak/Nie |
| System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora. | | Tak/Nie |
| **Intrusion Prevention System i Advanced Threat Protection** | | |
| Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur. | | Tak/Nie |
| Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS. | | Tak/Nie |
| System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet. | | Tak/Nie |
| System powinien posiadać mechanizm blokowania stron internetowych i adresów IP na bazie list. | | Tak/Nie |
| System blokowanie na bazie list powinien umożliwiać dodanie własnych list z adresami domen i adresami IP. | | Tak/Nie |
| System blokowanie na bazie list powinien umożliwiać automatyczną aktualizację list w interwale przynajmniej 3 razy dziennie. | | Tak/Nie |
| System blokowania na bazie list powinien umożliwiać dodawanie wyjątków. | | Tak/Nie |
| **Ochrona i kontrola web** | | |
| **Ochrona przez Malware** | | |
| Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP. | | Tak/Nie |
| Rozwiązanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania. | | Tak/Nie |
| Dodatkowo rozwiązanie powinno umożliwiać uruchomienie silnika antywirusowego firmy trzeciej. | | Tak/Nie |
| Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. | | Tak/Nie |
| System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. | | Tak/Nie |
| Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek. | | Tak/Nie |
| Rozwiązanie musi przeprowadzać emulację skryptów Java. | | Tak/Nie |
| Rozwiązanie powinno przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać blokowanie potencjalnie niechcianych aplikacji (tzw. Potentially Unwanted Applications - PUAs) | | Tak/Nie |
| System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates) | | Tak/Nie |
| **Inspecja ruchu SSL/TLS** | | |
| Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów. | | Tak/Nie |
| Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2. | | Tak/Nie |
| Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP. | | Tak/Nie |
| Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443). | | Tak/Nie |
| Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web. | | Tak/Nie |
| Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen. | | Tak/Nie |
| **Filtr Web** | | |
| Filtrowanie stron web powinno być oparte o predefiniowane kategorie z możliwością tworzenia własnych kategorii stron. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy. | | Tak/Nie |
| Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól. | | Tak/Nie |
| System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. | | Tak/Nie |
| Administrator powinien mieć możliwość modyfikowania treści komunikatu w tym dodania logo organizacji. | | Tak/Nie |
| **Ochrona i kontrola aplikacji** | | |
| Rozwiązanie powinno oferować bazę danych opisująca co najmniej 3000 aplikacji. | | Tak/Nie |
| Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji. | | Tak/Nie |
| Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać tworzenie własnych grup aplikacji co najmniej na potrzeby polityk SD-WAN. | | Tak/Nie |
| **Ochrona przed nieznanymi zagrożeniami** | | |
| Rozwiązanie klasy Sandbox do ochrony przez zagrożeniami typu Zero-Day. | | Tak/Nie |
| Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll. | | Tak/Nie |
| Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf. | | Tak/Nie |
| Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf. | | Tak/Nie |
| Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab. | | Tak/Nie |
| Rozwiązanie nie może mieć ograniczeń co do liczby analizowanych plików. | | Tak/Nie |
| System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS. | | Tak/Nie |
| System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu. | | Tak/Nie |
| System zapewniający ochronę przed exploitami i złośliwym kodem ransomware. | | Tak/Nie |
| System badający reputację pliku w zewnętrznych bazach takich jak np. Virustotal. | | Tak/Nie |
| System powinien oferować szczegółowe raporty dowodzące przeprowadzonej analizy dla w/w mechanizmów. | | Tak/Nie |
| **Subskrypcje** | | |
| Oferta musi zawierać subskrypcje dla wszystkich wymaganych modułów na okres nie krótszy niż 12 miesięcy | | Tak/Nie |
| **Gwarancja i wsparcie** | | |
| Wsparcie techniczne w trybie 8x5 na okres nie krótszy niż 12 miesięcy | | Tak/Nie |
| Gwarancja na sprzęt na okres nie krótszy niż 12 miesięcy | | Tak/Nie |
| Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. | | Tak/Nie |
| **Opis sposobu realizacja zadania:** | | |
| 1. Dostawa jednej sztuki urządzenia bezpieczeństwa sieci, montaż w szafie teletechnicznej, konfiguracja. Przez konfigurację urządzenia należy rozumieć: aktualizacja firmware do najnowszej wersji, założenie konta klienta dla nadzorowania urządzenia oraz licencji, wdrożenie podstawowych reguł firewall, reguł filtracji URL, reguł blokowania aplikacji, wdrożenie procesu backupu konfigurację urządzenia, wdrożenie logowania VPN (SSL VPN oraz IPSec). 2. Zamawiający wymaga, aby osoba przeprowadzająca konfigurację posiadała niezbędne kwalifikacje. | | Tak/Nie |

## **1.2 Urządzenie bezpieczeństwa sieci - 2 szt. (dla Ośrodka Pomocy Społecznej oraz Zakładu Gospodarki Komunalnej)**

**Marka: …………………………..**

**Model: …………………………..**

|  |  |  |
| --- | --- | --- |
| **Minimalne wymagania** | | **Parametr oferowany** |
| **System** | | |
| **Konstrukcja** | | |
| System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania. | | Tak/Nie |
| Rozwiązanie powinno być wyposażone w moduł kryptoraficzny zgodny ze standardem FIPS 140-2. | | Tak/Nie |
| Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca) | | Tak/Nie |
| Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie Active-Passive lub Active-Active. | | Tak/Nie |
| System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej. | | Tak/Nie |
| Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy (drugi zasilacz jako wyposażenie opcjonalne). | | Tak/Nie |
| Urządzenie w metalowej obudowie z możliwością montażu w szafie rack 19". | | Tak/Nie |
| Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB). | | Tak/Nie |
| Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie. | | Tak/Nie |
| Wbudowany port USB umożliwiający podłączenie pamięci flash i przeprowadzenie konfiguracji w trybie Zero Touch. | | Tak/Nie |
| Możliwość rozbudowy o dodatkowe moduły interfejsów sieciowych. | | Tak/Nie |
| Pamięć operacyjna RAM nie mniej niż (GB): | 8 | Tak/Nie |
| Przestrzeń do przechowywania logów i raportów nie mniej niż (GB) | 64 | Tak/Nie |
| Liczba fizycznych interfejsów 1000BASE-T nie mniej niż: | 9 | Tak/Nie |
| Liczba fizycznych interfejsów 1000BASE-X nie mniej niż: | 1 | Tak/Nie |
| Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q nie mniej niż: | 128 | Tak/Nie |
| **Wydajność** | | |
| Wydajność Firewall nie mniej niż (Mbps) | 15 000 | Tak/Nie |
| Wydajność Firewall IMIX nie mniej niż (Mbps) | 10 000 | Tak/Nie |
| Wydajność IPS nie mniej niż (Mbps) | 3 500 | Tak/Nie |
| Wydajność FW+IPS+AV nie mniej niż (Mbps) | 3 000 | Tak/Nie |
| Wydajność NGFW nie mniej niż (Mbps) | 3 500 | Tak/Nie |
| Liczba równoczesnych połączeń nie mniejsza niż: | 5 000 000 | Tak/Nie |
| Liczba nowych połączeń na sekundę nie mniejsza niż: | 60 000 | Tak/Nie |
| Wydajność IPsec VPN nie mniej niż (Mbps): | 10 000 | Tak/Nie |
| Liczba równoczesnych tuneli IPsec VPN nie mniejsza niż: | 1 000 | Tak/Nie |
| Liczba równoczesnych tuneli SSL VPN nie mniejsza niż: | 1 000 | Tak/Nie |
| Wydajność dla inspekcji ruchu SSL/TLS nie mniej niż (Mbps): | 1 000 | Tak/Nie |
| Liczba równoczesnych połączeń SSL/TLS nie mniejsza niż: | 15 000 | Tak/Nie |
| **Zarządzanie** | | |
| Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. | | Tak/Nie |
| Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). | | Tak/Nie |
| Rozwiązanie powinno oferować wsparcie dla generowania certyfikatów za pomocą firmy Let’s Encrypt. | | Tak/Nie |
| Rozwiązanie powinno oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. | | Tak/Nie |
| Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter. | | Tak/Nie |
| Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. | | Tak/Nie |
| Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. | | Tak/Nie |
| System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. | | Tak/Nie |
| System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. | | Tak/Nie |
| System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. | | Tak/Nie |
| Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). | | Tak/Nie |
| System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. | | Tak/Nie |
| Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). | | Tak/Nie |
| System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog). | | Tak/Nie |
| Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej. | | Tak/Nie |
| System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS). | | Tak/Nie |
| Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta. | | Tak/Nie |
| System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpowiednik). | | Tak/Nie |
| System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia. | | Tak/Nie |
| System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta. | | Tak/Nie |
| Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji z zapisem do pliku na komputer administratora, na serwer FTP, lub na email. | | Tak/Nie |
| Rozwiązanie powinno oferować wbudowany mechanizm pozwalający na automatyczne tworzenie szyfrowanych hasłem kopii zapasowych konfiguracji w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu. | | Tak/Nie |
| Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich. | | Tak/Nie |
| Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). Informacja o dostępności nowej wersji powinna pojawiać się w Web GUI. | | Tak/Nie |
| Producent powinien oferować mechanizm automatycznego łatania wykrytych w oprogramowaniu systemowym podatności przez tzw. hotfixies, przy czym administrator powinien móc funkcjonalność tą wyłączyć. | | Tak/Nie |
| **Zapora sieciowa, konfiguracja sieciowa oraz routing** | | |
| **Zapora sieciowa** | | |
| Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection. | | Tak/Nie |
| System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas. | | Tak/Nie |
| System powinien pozwalać na selektywne wyłączanie reguł zapory sieciowej (bez konieczności ich usuwania). | | Tak/Nie |
| System powinien pozwalać na grupowanie reguł zapory. Wymagana jest funkcjonalność automatycznego wiązania nowotworzonych reguł do właściwych grup na podstawie kryteriów opisujących grupę. | | Tak/Nie |
| Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. | | Tak/Nie |
| System ochrony powinien zawierać predefiniowane strefy zapory typu: LAN, WAN, DMZ, VPN. | | Tak/Nie |
| Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej. | | Tak/Nie |
| System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). | | Tak/Nie |
| Rozwiązanie powinno oferować narzędzie do symulowanego testu reguł zapory w oparciu o zadane przez administratora kryteria takie jak IP, strefa zapory, użytkownik, dzień, godzina. | | Tak/Nie |
| **Trasowanie ruchu** | | |
| Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing. | | Tak/Nie |
| Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. | | Tak/Nie |
| Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać rozkładanie ruchu w oparciu o wagi interfejsów WAN. | | Tak/Nie |
| Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast. | | Tak/Nie |
| Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). | | Tak/Nie |
| Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM). | | Tak/Nie |
| Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6. | | Tak/Nie |
| **Translacja adresów i portów** | | |
| Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT. | | Tak/Nie |
| Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT | | Tak/Nie |
| Rozwiązanie powinno pozwalać na automatyczne tworzenie reguł NAT typu loopback czy reflexive rule. | | Tak/Nie |
| **Kształtowanie pasma i jakość usług** | | |
| System powinien zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji. | | Tak/Nie |
| Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne. | | Tak/Nie |
| System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. | | Tak/Nie |
| Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6. | | Tak/Nie |
| Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet. | | Tak/Nie |
| **Podstawowa ochrona przed atakami DoS i DDoS** | | |
| System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection). | | Tak/Nie |
| **Pozostałe** | | |
| Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. | | Tak/Nie |
| Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge). | | Tak/Nie |
| System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. | | Tak/Nie |
| System powinien oferować wsparcie dla IEEE 802.3Q VLAN z możliwością konfiguracji niezależnych puli DHCP. | | Tak/Nie |
| Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). | | Tak/Nie |
| System powinien oferować wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp. | | Tak/Nie |
| Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd). | | Tak/Nie |
| Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo). | | Tak/Nie |
| Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych. | | Tak/Nie |
| **Uwierzytelnianie i obsługa użytkowników** | | |
| Wymagane uwierzytelnianie użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta. | | Tak/Nie |
| Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników. | | Tak/Nie |
| System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory. | | Tak/Nie |
| System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm). | | Tak/Nie |
| Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server. | | Tak/Nie |
| System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. | | Tak/Nie |
| Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu. | | Tak/Nie |
| **Koncentrator VPN** | | |
| System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2. | | Tak/Nie |
| System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519). | | Tak/Nie |
| System musi obsługiwać połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN. | | Tak/Nie |
| Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN. | | Tak/Nie |
| Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback. | | Tak/Nie |
| Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego. | | Tak/Nie |
| Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth. | | Tak/Nie |
| Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połaczeń IPsec client-to-site VPN jak i SSL client-to-site VPN. | | Tak/Nie |
| Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN. | | Tak/Nie |
| Urządzenie musi obsługiwać połączenia L2TP over IPsec. | | Tak/Nie |
| **Logowanie i raportowanie** | | |
| System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym. | | Tak/Nie |
| System powinien umożliwiać składowanie oraz archiwizację logów. | | Tak/Nie |
| Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. | | Tak/Nie |
| Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów. | | Tak/Nie |
| Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa. | | Tak/Nie |
| System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali. | | Tak/Nie |
| System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać wysyłanie raportów via email. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV. | | Tak/Nie |
| Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog. | | Tak/Nie |
| System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza. | | Tak/Nie |
| System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację. | | Tak/Nie |
| Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach. | | Tak/Nie |
| System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora. | | Tak/Nie |
| **Intrusion Prevention System i Advanced Threat Protection** | | |
| Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur. | | Tak/Nie |
| Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS. | | Tak/Nie |
| System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet. | | Tak/Nie |
| System powinien posiadać mechanizm blokowania stron internetowych i adresów IP na bazie list. | | Tak/Nie |
| System blokowanie na bazie list powinien umożliwiać dodanie własnych list z adresami domen i adresami IP. | | Tak/Nie |
| System blokowanie na bazie list powinien umożliwiać automatyczną aktualizację list w interwale przynajmniej 3 razy dziennie. | | Tak/Nie |
| System blokowania na bazie list powinien umożliwiać dodawanie wyjątków. | | Tak/Nie |
| **Ochrona i kontrola web** | | |
| **Ochrona przez Malware** | | |
| Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP. | | Tak/Nie |
| Rozwiązanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania. | | Tak/Nie |
| Dodatkowo rozwiązanie powinno umożliwiać uruchomienie silnika antywirusowego firmy trzeciej. | | Tak/Nie |
| Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. | | Tak/Nie |
| System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. | | Tak/Nie |
| Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek. | | Tak/Nie |
| Rozwiązanie musi przeprowadzać emulację skryptów Java. | | Tak/Nie |
| Rozwiązanie powinno przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać blokowanie potencjalnie niechcianych aplikacji (tzw. Potentially Unwanted Applications - PUAs) | | Tak/Nie |
| System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates) | | Tak/Nie |
| **Inspecja ruchu SSL/TLS** | | |
| Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów. | | Tak/Nie |
| Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2. | | Tak/Nie |
| Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP. | | Tak/Nie |
| Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443). | | Tak/Nie |
| Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web. | | Tak/Nie |
| Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen. | | Tak/Nie |
| **Filtr Web** | | |
| Filtrowanie stron web powinno być oparte o predefiniowane kategorie z możliwością tworzenia własnych kategorii stron. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy. | | Tak/Nie |
| Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól. | | Tak/Nie |
| System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. | | Tak/Nie |
| Administrator powinien mieć możliwość modyfikowania treści komunikatu w tym dodania logo organizacji. | | Tak/Nie |
| **Ochrona i kontrola aplikacji** | | |
| Rozwiązanie powinno oferować bazę danych opisująca co najmniej 3000 aplikacji. | | Tak/Nie |
| Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji. | | Tak/Nie |
| Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp. | | Tak/Nie |
| Rozwiązanie powinno umożliwiać tworzenie własnych grup aplikacji co najmniej na potrzeby polityk SD-WAN. | | Tak/Nie |
| **Ochrona przed nieznanymi zagrożeniami** | | |
| Rozwiązanie klasy Sandbox do ochrony przez zagrożeniami typu Zero-Day. | | Tak/Nie |
| Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll. | | Tak/Nie |
| Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf. | | Tak/Nie |
| Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf. | | Tak/Nie |
| Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab. | | Tak/Nie |
| Rozwiązanie nie może mieć ograniczeń co do liczby analizowanych plików. | | Tak/Nie |
| System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS. | | Tak/Nie |
| System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu. | | Tak/Nie |
| System zapewniający ochronę przed exploitami i złośliwym kodem ransomware. | | Tak/Nie |
| System badający reputację pliku w zewnętrznych bazach takich jak np. Virustotal. | | Tak/Nie |
| System powinien oferować szczegółowe raporty dowodzące przeprowadzonej analizy dla w/w mechanizmów. | | Tak/Nie |
| **Subskrypcje** | | |
| Oferta musi zawierać subskrypcje dla wszystkich wymaganych modułów na okres nie krótszy niż 12 miesięcy | | Tak/Nie |
| **Gwarancja i wsparcie** | | |
| Wsparcie techniczne w trybie 8x5 na okres nie krótszy niż 12 miesięcy | | Tak/Nie |
| Gwarancja na sprzęt na okres nie krótszy niż 12 miesięcy | | Tak/Nie |
| Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. | | Tak/Nie |
| **Opis sposobu realizacja zadania:** | | |
| * Dostawa dwóch sztuk urządzenia bezpieczeństwa sieci, montaż w szafie teletechnicznej, konfiguracja. Przez konfigurację urządzenia należy rozumieć: aktualizacja firmware do najnowszej wersji, założenie konta klienta dla nadzorowania urządzenia oraz licencji, wdrożenie podstawowych reguł firewall, reguł filtracji URL, reguł blokowania aplikacji, wdrożenie procesu backupu konfigurację urządzenia, wdrożenie logowania VPN (SSL VPN oraz IPSec).  1. Zamawiający wymaga, aby osoba przeprowadzająca konfigurację posiadała niezbędne kwalifikacje. | | Tak/Nie |

# **2. Dostawa, montaż, konfiguracja trzech sztuk urządzeń magazynujących dane (urządzenia NAS) dla Urzędu Gminy Ożarowice, Ośrodka Pomocy Społecznej, Zakładu Gospodarki Komunalnej**

## **2.1 Urządzenie magazynujące dane (NAS) – 2 szt. (dla Urzędu Gminy Ożarowice oraz dla Ośrodka Pomocy Społecznej)**

**Marka: …………………………..**

**Model: …………………………..**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimalne wymagania** | **Parametr oferowany** |
| Procesor | Wielordzeniowy procesor osiągający wynik minimum 5200 punktów w teście PassMark. | Tak/Nie |
| Obudowa | Typu rack 19’’ o wysokości maksymalnie 1U wraz z szynami przesuwnymi umożliwiającymi montaż w szafie rack w zestawie. | Tak/Nie |
| Pamięć RAM | Minimum 16GB ECC UDIMM z możliwością rozbudowy do 64GB. Nie zezwala się na stosowanie zamienników pamięci RAM. | Tak/Nie |
| Ilość obsługiwanych dysków | Minimum 4 dyski o maksymalnej pojemności nie mniejszej niż 18TB każdy,  po podłączeniu modułów rozszerzających minimum 16 dysków. | Tak/Nie |
| Zainstalowane dyski | Minimum 4 dyski o pojemności 8TB każdy zgodne z listą kompatybilności oferowanego serwera oraz charakteryzujące się następującymi parametrami: - interfejs: SATA 6Gb/s,  - prędkość obrotowa: minimum 7200 RPM,  - gwarancja: minimum 60 miesięcy,  - MTBF: minimum 2 miliony. | Tak/Nie |
| Interfejsy sieciowe | Minimum 4 porty 1GbE RJ-45. | Tak/Nie |
| Porty | Minimum 2 porty USB 3.2. Minimum 1 gniazdo rozszerzenia służące do podłączania jednostek rozszerzających. | Tak/Nie |
| Wskaźniki LED | Status, HDD, zasilanie, LAN | Tak/Nie |
| Obsługa RAID | Podstawowy, RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare. | Tak/Nie |
| Funkcje RAID | Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5. | Tak/Nie |
| Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych. | Tak/Nie |
| Protokoły | SMB, NFS, FTP, WebDAV, iSCSI, SSH, SNMP | Tak/Nie |
| Usługi | 1. Serwer VPN, Windows ACL, Integracja z Windows Active Directory, Firewall, Serwer WWW, Serwer plików, Manager plików przez WebUI, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki, możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów.  2. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 10 lub nowszym według harmonogramu z możliwością zarządzania z poziomu centralnej konsoli dostępnej lokalnie oraz zdalnie, przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Dane z kopii zapasowych muszą być redukowane poprzez globalną deduplikację po stronie miejsca przechowywania. Licencja musi umożliwiać podłączanie kolejnych komputerów do systemu kopii zapasowej bez limitu.  3. Możliwość utworzenia klastra wysokiej dostępności (ang. High Availability Cluster) pracującego minimum w trybie aktywny - pasywny. Klaster musi obsługiwać w pełni automatyczne przełączanie awaryjne bez ingerencji administratora. W skład klastra muszą wchodzić co najmniej 2 urządzenia. Wymagane jest, aby klaster mógł zostać skonfigurowany w oparciu o dwa identyczne modele oraz dwa różne, ale podobne sprzętowo modele. | Tak/Nie |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów. | Tak/Nie |
| Język GUI | Polski | Tak/Nie |
| Gwarancja i serwis | Minimum 24 miesiące gwarancji świadczonej przez producenta lub autoryzowanego partnera serwisowego producenta oferowanego rozwiązania, działającej w trybie 5/13 NBD na cały system złożony z serwera, dysków i akcesoriów z opcją pozostawienia uszkodzonego nośnika u Zamawiającego. Wydłużenie okresu gwarancji jest jednym z kryteriów oceny składanej oferty (opis w SWZ). | Gwarancja oferowana:  … lat/a |
| Waga bez dysków | Maksymalnie 15 kg | Tak/Nie |
| Typowy pobór mocy podczas pracy | Maksymalnie 400W | Tak/Nie |
| Certyfikaty | CE, FCC lub równoważne | Tak/Nie |
| System plików | Dyski wewnętrzne: BTRFS lub inny równoważny | Tak/Nie |
| Szyfrowanie | Mechanizm szyfrowania sprzętowego | Tak/Nie |
| Zasilacz | Redundantny zasilacz o mocy pozwalającej na bezproblemową pracę w przypadku awarii jednego modułu zasilacza. | Tak/Nie |
| Chłodzenie | Minimum 2 wentylatory z możliwością regulowania prędkości obrotowej. | Tak/Nie |
| Opis sposobu realizacja zadania: | Dostawa dwóch sztuk urządzenia NAS, montaż w szafie teletechnicznej, konfiguracja. Przez konfigurację urządzenia należy rozumieć: aktualizacja firmware do najnowszej wersji. | Tak/Nie |

## **2.2 Urządzenie magazynujące dane (NAS) – 1 szt. (dla Zakładu Gospodarki Komunalnej)**

**Marka: …………………………..**

**Model: …………………………..**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimalne wymagania** | **Parametr oferowany** |
| Procesor | Wielordzeniowy procesor osiągający wynik minimum 5200 punktów w teście PassMark. | Tak/Nie |
| Obudowa | Typu rack 19’’ o wysokości maksymalnie 1U wraz z szynami przesuwnymi umożliwiającymi montaż w szafie rack w zestawie. | Tak/Nie |
| Pamięć RAM | Minimum 16GB ECC UDIMM z możliwością rozbudowy do 64GB. Nie zezwala się na stosowanie zamienników pamięci RAM. | Tak/Nie |
| Ilość obsługiwanych dysków | Minimum 4 dyski o maksymalnej pojemności nie mniejszej niż 18TB każdy,  po podłączeniu modułów rozszerzających minimum 16 dysków. | Tak/Nie |
| Zainstalowane dyski | Minimum 2 dyski o pojemności 16TB każdy zgodne z listą kompatybilności oferowanego serwera oraz charakteryzujące się następującymi parametrami: - interfejs: SATA 6Gb/s,  - prędkość obrotowa: minimum 7200 RPM,  - gwarancja: minimum 60 miesięcy,  - MTBF: minimum 2 miliony. | Tak/Nie |
| Interfejsy sieciowe | Minimum 4 porty 1GbE RJ-45. | Tak/Nie |
| Porty | Minimum 2 porty USB 3.2. Minimum 1 gniazdo rozszerzenia służące do podłączania jednostek rozszerzających. | Tak/Nie |
| Wskaźniki LED | Status, HDD, zasilanie, LAN | Tak/Nie |
| Obsługa RAID | Podstawowy, RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare. | Tak/Nie |
| Funkcje RAID | Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5. | Tak/Nie |
| Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych. | Tak/Nie |
| Protokoły | SMB, NFS, FTP, WebDAV, iSCSI, SSH, SNMP | Tak/Nie |
| Usługi | 1. Serwer VPN, Windows ACL, Integracja z Windows Active Directory, Firewall, Serwer WWW, Serwer plików, Manager plików przez WebUI, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki, możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów.  2. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 10 lub nowszym według harmonogramu z możliwością zarządzania z poziomu centralnej konsoli dostępnej lokalnie oraz zdalnie, przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Dane z kopii zapasowych muszą być redukowane poprzez globalną deduplikację po stronie miejsca przechowywania. Licencja musi umożliwiać podłączanie kolejnych komputerów do systemu kopii zapasowej bez limitu.  3. Możliwość utworzenia klastra wysokiej dostępności (ang. High Availability Cluster) pracującego minimum w trybie aktywny - pasywny. Klaster musi obsługiwać w pełni automatyczne przełączanie awaryjne bez ingerencji administratora. W skład klastra muszą wchodzić co najmniej 2 urządzenia. Wymagane jest, aby klaster mógł zostać skonfigurowany w oparciu o dwa identyczne modele oraz dwa różne, ale podobne sprzętowo modele. | Tak/Nie |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów. | Tak/Nie |
| Język GUI | Polski | Tak/Nie |
| Gwarancja i serwis | Minimum 24 miesiące gwarancji świadczonej przez producenta lub autoryzowanego partnera serwisowego producenta oferowanego rozwiązania, działającej w trybie 5/13 NBD na cały system złożony z serwera, dysków i akcesoriów z opcją pozostawienia uszkodzonego nośnika u Zamawiającego. | Gwarancja oferowana:  … lat/a |
| Waga bez dysków | Maksymalnie 15 kg | Tak/Nie |
| Typowy pobór mocy podczas pracy | Maksymalnie 400W | Tak/Nie |
| Certyfikaty | CE, FCC lub równoważne | Tak/Nie |
| System plików | Dyski wewnętrzne: BTRFS lub inny równoważny | Tak/Nie |
| Szyfrowanie | Mechanizm szyfrowania sprzętowego | Tak/Nie |
| Zasilacz | Redundantny zasilacz o mocy pozwalającej na bezproblemową pracę w przypadku awarii jednego modułu zasilacza. | Tak/Nie |
| Chłodzenie | Minimum 2 wentylatory z możliwością regulowania prędkości obrotowej. | Tak/Nie |
| Opis sposobu realizacja zadania | Dostawa jednej sztuki urządzenia NAS, montaż w szafie teletechnicznej, konfiguracja. Przez konfigurację urządzenia należy rozumieć: aktualizacja firmware do najnowszej wersji. | Tak/Nie |

# **3. Dostawa, montaż trzech sztuk zasilaczy awaryjnych (UPS) dla Urzędu Gminy Ożarowice, Ośrodka Pomocy Społecznej, Zakładu Gospodarki Komunalnej.**

**Marka: …………………………..**

**Model: …………………………..**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimalne wymagania** | **Parametr oferowany** |
| Minimalne wymagania techniczne dla jednostki UPS | Moc znamionowa jednostki nie mniej niż 2700W/3000VA  Wersja do montażu w szafie rack 19’’  Technologia Line Interactive  Temperatura eksploatacji 0 - 40 °C  Wilgotność względna podczas pracy 0 - 95 %  Wysokość n.p.m. podczas pracy 0 – 3000m  Hałas słyszalny w odległości 1 m od powierzchni urządzenia 55.0 dBA  Rozpraszanie ciepła w trybie online 348.0BTU/godz.  Klasa energetyczna sprzętu przeciwprzepięciowego 320J | Tak/Nie |
| Parametry wejściowe | Nominalne napięcie wejściowe 230V  Częstotliwość wejściowa 50/60 Hz +/-3 Hz (automatyczne wykrywanie)  Typ gniazda wejściowego:  - IEC 320 C20,  Zmienny zakres napięcia wejściowego w trybie podstawowym 160 - 286V (max zakres: 150 - 300 V) | Tak/Nie |
| Parametry wyjściowe | Napięcie wyjściowe 230V  Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz ±3Hz  Inne napięcia wyjściowe 220, 240V  Typ przebiegu sinusoida  Złącza/gniazda wyjściowe  (8) IEC 320 C13  (1) IEC 320 C19 | Tak/Nie |
| Akumulatory i czas podtrzymania | Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny  Czas autonomii:  3 minuty dla pełnego obciążenia  11 minut dla połowy obciążenia  Typowy czas ładowania 3 godziny  Oczekiwana żywotność akumulatora (lata) 3 – 5  Akumulatory wymieniane na gorąco  Automatyczny test akumulatora | Tak/Nie |
| Komunikacja i zarządzanie | Gniazdo do montażu karty WEB/SNMP-Smart Slot x1  Wstępnie zainstalowana karta zarządzania siecią do monitorowania i zarządzania UPS. Czujnik temperatury dostarczony w zestawie z UPS.  Karta posiada port uniwersalny do podłączenia np. czujnika temperatury  Porty komunikacyjne: Serial (RJ-45), SmartSlot, USB  Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD.  Alarm dźwiękowy: Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia  Awaryjny wyłącznik zasilania (EPO) Tak | Tak/Nie |
| Certyfikaty, zgodności oraz gwarancja | CE, EN62040-1, EN62040-2, VDE, RoHS, REACh lub równoważne  3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulator | Tak/Nie |
| Oprogramowanie z którym współpracuje  zasilacz | Dostępne oprogramowanie zasilacza do zarządzania/monitoringu (niektóre wersje odpłatne) wspołpracuje z Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2025 2025);Red Hat® Enterprise Linux; SuSE® Linux®. | Tak/Nie |
| Opis sposobu realizacja zadania | Dostawa trzech sztuk zasilaczy awaryjnych (UPS), montaż w szafie teletechnicznej, konfiguracja. Przez konfigurację urządzenia należy rozumieć aktualizację firmware do najnowszej wersji. | Tak/Nie |

# **4. Dostawa, montaż, dwóch sztuk serwerów z oprogramowaniem, dla Ośrodka Pomocy Społecznej oraz Zakładu Gospodarki Komunalnej.**

**Marka: …………………………..**

**Model: …………………………..**

**Minimalne wymagane parametry serwera**

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimalne wymagania** | **Parametr oferowany** |
| **Obudowa** | * Typu RACK 19”, wysokość 1U; * Szyny umożliwiające wysunięcie serwera z szafy stelażowej; * Możliwość zainstalowania 8 dysków twardych hot plug 2,5”; * Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych; * Zainstalowane 2 szt. dysków SSD 960GB Hot-Plug DWPD nie mniejsze niż 5; * Możliwość zainstalowania dysku M.2 NVMe bezpośrednio na płycie głównej; * Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray. | Tak/Nie |
| **Płyta główna** | * Wyprodukowana i zaprojektowana przez producenta serwera; * Możliwość instalacji procesorów 8-rdzeniowych; * Zainstalowany moduł TPM 2.0; * Złącza PCI Express: * 2 fizyczne złącza PCIe 5.0 o prędkości x8; * Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości; * 4 gniazda pamięci RAM; * Obsługa minimum 128 GB pamięci RAM DDR5 ECC; * Możliwość instalacji 2 dysków M.2 NVMe skonfigurowanych w RAID-1 na płycie głównej lub dedykowanej karcie PCI Express, dyski nie mogą zajmować klatek dla dysków hot-plug. | Tak/Nie |
| **Procesory** | * Jeden procesor 8-rdzeniowy, taktowanie bazowe 3 GHz, architektura x86\_64; osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 108 pkt | Tak/Nie |
| **Pamięć RAM** | * 64 GB pamięci RAM; * Pamięci obsadzone w trybie dwukanałowym; | Tak/Nie |
| **Kontrolery LAN** | Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:   * 2x 1Gbit Base-T;   Interfejsy LAN zainstalowane w slotach PCI-e:   * 2x 1Gbit Base-T; | Tak/Nie |
| **Kontrolery I/O** | * Kontroler SAS RAID dla dysków wewnętrznych posiadający 2GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania; | Tak/Nie |
| **Porty** | * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; * 4x USB 3.2 Gen1 Type A wyprowadzone na tył obudowy * 2x USB 3.2 Gen1 Type A + 1x USB3.2 Gen2x2 Type C wyprowadzone na przód obudowy * 5x SATA 6G * Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem; * Ilość dostępnych złącz USB/SATA nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera. | Tak/Nie |
| **Zasilanie, chłodzenie** | * Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 500W; * Redundantne wentylatory hotplug. | Tak/Nie |
| **Zarządzanie** | * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii; * informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: * karty rozszerzeń zainstalowane w dowolnym slocie PCI Express; * procesory CPU; * pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM; * status karty zarządzającej serwera; * wentylatory; * bateria podtrzymująca ustawienia BIOS płyty głównej; * zasilacze; * Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: * Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; * Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; * Dostęp poprzez przeglądarkę Web, SSH; * Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; * Zarządzanie alarmami (zdarzenia poprzez SNMP); * Możliwość przejęcia konsoli tekstowej; * Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); * Obsługa serwerów proxy (autentykacja); * Obsługa VLAN; * Możliwość konfiguracji parametru Max. Transmission Unit (MTU); * Wsparcie dla protokołu SSDP; * Obsługa protokołów TLS 1.2, SSL v3; * Obsługa protokołu LDAP; * Integracja z HP SIM; * Synchronizacja czasu poprzez protokół NTP; * Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej; * Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); * Wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; * Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. | Tak/Nie |
| **Wspierane/Certyfikowane OS** | * Microsoft Windows Server 2022, Microsoft Windows Server 2025; * VMWare vSphere 8.0; * Suse Linux Enterprise Server 15; * Red Hat Enterprise Linux 9, 8; * Ubuntu 22.04, Ubuntu 24.04 | Tak/Nie |
| **Gwarancja** | Minimum 2 lata gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika serwisu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej. **Wydłużenie okresu gwarancji jest jednym z kryteriów oceny składanej oferty (opis w SWZ).**   * Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; * Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych lub certyfikat równoważny; * Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; * Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty). | Gwarancja oferowana:  … lat/a |
| **Dokumentacja, inne** | * Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta; * Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; * Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera; * W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; * Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; * Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 85 %; * Zgodność z normami: CB, RoHS, WEEE oraz CE lub równoważne | Tak/Nie |
| **Opis sposobu realizacja zadania** | Dostawa dwóch sztuk serwerów z oprogramowaniem Windows Server 2025 Standard 16Core ROK \_ WINSVR CAL 2025 15Use (zamawiający wymaga powyższy system operacyjny ze względu na posiadane i wykorzystywane oprogramowanie, które zostało zaprojektowane i działa wyłącznie w ww. środowisku operacyjnym), montaż w szafie teletechnicznej. | Tak/Nie |

# **5.** **Przedłużenie licencji oprogramowania dla Urzędu Gminy Ożarowice**

## **5.1. Przedłużenie licencji oprogramowania - skaner podatności WithSecure Elements Exposure Management for Users – 40 użytkowników**

**Dostawa licencji oprogramowania skanera podatności**

Celem dostawy jest budowa zintegrowanego **w jednej konsoli zarządzającej** systemu bezpieczeństwa i nadzoru nad komputerami serwerami oraz urządzeniami sieciowymi. Ze względu na to że zamawiający posiada już wdrożone rozwiązanie **WithSecure Elements** w zakresie ochrony antywirusowej (instalacja agentów na komputerach i serwerach, wdrożenie profili ochrony, kontrola nośników danych, raportowanie itd.), wymaga się przedłużenia licencji.

**WithSecure Elements Exposure Management for Users – 40 użytkowników**

**Opis sposobu realizacja zadania**

1. licencja ważna do 30.06.2026 r.
2. uruchomienie licencji na koncie klienta
3. przekazanie licencji (forma papierowa lub wersja elektroniczna)
4. szkolenie stacjonarne (min. 4 godziny) na miejscu w siedzibie klienta w zakresie w/w produktu

Zamawiający wymaga, aby osoba przeprowadzająca szkolenie posiadała kwalifikacje potwierdzone certyfikatami:

* certyfikat - EXM Tech Basic - WithSecure Elements Exposure Management Technical Training (Basic)
* certyfikat - XM Tech Advanced (Vulnerabilities) - WithSecure Elements Exposure Management for Business Technical Training (Advanced)

lub certyfikatami równoważnymi.

Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 (lub równoważny), w szczególności w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.

Oferent winien przedłożyć dokumenty (w trakcie realizacji zamówienia):

* Oświadczanie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
* Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego (lub certyfikat równoważny).

## **5.2. Przedłużenie licencji posiadanego oprogramowania do cyberochrony (backup, odzyskiwanie danych) Acronis Cyber Protect Cloud – 40 użytkowników**

**Opis sposobu realizacja zadania**

- licencja ważna do 30.06.2026 r.

- odnowienie licencji na koncie klienta

- przekazanie odnowienia licencji (forma papierowa lub wersja elektroniczna)

Odnowienie licencji posiadanego już rozwiązania kopii danych z konsolą w chmurze dla 40stacji roboczych

**Uwagi**

1. *Specyfikacja techniczna oferowanego sprzętu stanowi treść oferty i pod rygorem odrzucenia oferty musi:*
   1. *zostać złożona wraz z ofertą;*
   2. *zostać podpisana przez Wykonawcę podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym;*
   3. *zostać wypełniona w zakresie rozdziałów 1-4;*
   4. *wskazywać markę i model oferowanego sprzętu.*
2. *W przypadku konieczności zaznaczenia opcji „tak” albo „nie” należy skreślić albo usunąć niewłaściwą odpowiedź.*
3. *W przypadku nieuzupełnienia informacji w zakresie oferowanych parametrów Zamawiający przyjmie, że Wykonawca oferuje minimalny parametr wymagany przez Zamawiającego określony w kolumnie „Minimalne wymagania”. Zastrzeżenie to dotyczy wyłącznie parametrów, dla których należy odpowiedzieć „tak” albo „nie”.*