**Formularz wymogów**

**Załącznik nr 2a swz**

Znak Sprawy: **PCM/ZP 09/I/2022**

**Nazwa Wykonawcy...................................................................................................................**

**Adres:..........................................................................................................................................**

**NIP:............................................................................REGON..................................................**

**OPIS PRZEDMIOTU ZAMÓWIENIA – WYMAGANIA SPRZĘTOWE**

Zakup i dostawa sprzętu sieciowego typu UTM

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymaganie | Wymagane bezwzględnie | Spełnienie przez OferentaTAK/NIE |
| 1. | **Wymagania Ogólne**Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.System musi wspierać IPv4 oraz IPv6 w zakresie:* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.
 | TAK |  |
| 2. | **Redundancja, monitoring i wykrywanie awarii**W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.Monitoring stanu realizowanych połączeń VPN. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. | TAK |  |
|  | **Interfejsy, Dysk, Zasilanie**1. System realizujący funkcję Firewall musi dysponować minimum:
* 16 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 2 gniazdami SFP+ 10 Gbps.
1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w zasilanie AC.
 | TAK |  |
|  | **Parametry wydajnościowe**W zakresie Firewall’a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps. | TAK |  |
|  | **Funkcje Systemu Bezpieczeństwa**W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.Kontrola Aplikacji. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.Ochrona przed atakami - Intrusion Prevention System.Kontrola stron WWW. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.Zarządzanie pasmem (QoS, Traffic shaping).Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.Analiza ruchu szyfrowanego protokołem SSH.Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system | TAK |  |
|  | **Polityki, Firewall**1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.* Amazon Web Services (AWS).
* Microsoft Azure
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
 | TAK |  |
|  | **Połączenia VPN**1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:Wsparcie dla IKE v1 oraz v2.Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).Obsługa protokołu Diffie-Hellman grup 19 i 20.Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.Mechanizm „Split tunneling” dla połączeń Client-to-Site.2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. | TAK |  |
|  | **Routing i obsługa łączy WAN**W zakresie routingu rozwiązanie powinno zapewniać obsługę:Routingu statycznego.Policy Based Routingu.Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. | TAK |  |
|  | **Funkcje SD-WAN**1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
 | TAK |  |
|  | **Zarządzanie pasmem**1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. | TAK |  |
|  | **Ochrona przed malware**Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.  | TAK |  |
|  | **Ochrona przed atakami**Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.Wykrywanie i blokowanie komunikacji C&C do sieci botnet. | TAK |  |
|  | **Kontrola aplikacji**1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
 | TAK |  |
|  | **Kontrola WWW**1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. | TAK |  |
|  | **Uwierzytelnianie użytkowników w ramach sesji**1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. | TAK |  |
|  | **Zarządzanie**1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. | TAK |  |
|  | **Logowanie**1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.Musi istnieć możliwość logowania do serwera SYSLOG. | TAK |  |
|  | **Certyfikaty**Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:* ICSA lub EAL4 dla funkcji Firewall.
 | TAK |  |
|  | **Serwisy i licencje**W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [36] miesięcy.  | TAK |  |
|  | **Gwarancja oraz wsparcie**1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres [36] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
* Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
* Certyfikat ISO 9001 podmiotu serwisującego.
 | TAK |  |

Zakup i dostawa przełączników sieciowych

Przełącznik sieciowy (24-port) – 4 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymaganie | Wymagane bezwzględnie | Spełnienie przez OferentaTAK/NIE |
|  | **Porty:*** Minimum 24 porty 1G RJ45 10/100/1000Mbit BASE-T wspierające zasilanie PoE w standardach IEEE 802.3 af, 802.3 at
* Minimum 4 porty SFP+ z możliwością pracy 1G/10GbE

Porty SFP+ muszą umożliwiać ich obsadzanie wkładkami 10 Gigabit Ethernet – minimum 10GBase-SR, LR, oraz Gigabit Ethernet – minimum 1000Base- SX, 1000Base LX | TAK |  |
|  | **Parametry fizyczne:**Wysokość maksymalnie 1U,montowany w szafie typu rack 19’’ | TAK |  |
|  | **Pamięć:*** Co najmniej 512 MB SDRAM

Co najmniej 256 MB pamięci flashBufor pakietów co najmniej 1.5 MB | TAK |  |
|  | **Procesor:**min. CPU ARM Cortex-A9 @ 800 MHz | TAK |  |
|  | **Wielkość tablicy adresów MAC:** co najmniej 16000 | TAK |  |
|  | **Ilość obsługiwanych sieci VLAN: b**o najmniej 256 | TAK |  |
|  | **Wydajność:** • Przepustowość przełączania: min. 128 Gbit/s • Przełączanie dla pakietów: min. 95.23 Mpps. • Opóźnienie:* < 4.7 uSec dla 100 Mb

< 2.4 uSec dla 1000 Mb<1.3 uSec dla 10 Gbps**Obsługa ramek Jumbo o wielkości co najmniej 9216 bajtów** | TAK |  |
|  | **Funkcjonalność urządzenia*** obsługa agregacji portów zgodnie z LACP (IEEE 802.3ad),

obsługa protokołu SNTP,Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), MSTP (802.1s)Minimum 256 obsługiwanych sieci VLANAutomatyczne przydzielanie klasy urządzenia PoE w oparciu o LLDP oraz LLDP-MED.Minimum 50 możliwych do utworzenia list ACL,CoS zgodna z 802.1pVoice VLANMinimum 509 wpisów ARPMożliwość przechowywania dwóch obrazów oprogramowania: aktywny i zapasowyPort SecurityDHCP SnoopingKlient RadiusPort mirroring,DHCP Relay,DoS Protection,ARP Attack Protection,Możliwość utworzenia minimum 32 statycznych wpisów w tablicy routingu | TAK |  |
|  | **Zasilanie**: zasilacz 230V AC wbudowany, | TAK |  |
|  | **Temperatura pracy**: 0°C do 40°C | TAK |  |
|  | **Maksymalny pobór mocy**: 234 W | TAK |  |
|  | **Maksymalny budżet mocy PoE** wynosi 195W (PoE klasy 4) | TAK |  |
|  | **Zarządzanie**: WWW (GUI), SNMP Manager, cloud-based web portal | TAK |  |
|  | **Gwarancja:** min. 5 lat + 5 lat od daty wycofania produktu ze sprzedaży | TAK |  |
|  | **Wykonawca winien przedłożyć dokumenty*** Deklaracja zgodności CE oferowanego urządzenia – certyfikat potwierdzony za zgodność z oryginałem,

Oświadczenie producenta lub oświadczenie autoryzowanego przedstawiciela producenta potwierdzające zgodność wszystkich parametrów oferowanego urządzenia wskazanych w Opisie przedmiotu zamówienia. | TAK |  |

Przełącznik sieciowy (48-port) – 4 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymaganie | Wymagane bezwzględnie | Spełnienie przez OferentaTAK/NIE |
|  | **Porty** :* Minimum 48 porty 1G RJ45 10/100/1000Mbit BASE-T wspierające zasilanie PoE w standardach IEEE 802.3 af, 802.3 at
* Minimum 4 porty SFP+ z możliwością pracy 1G/10GbE

Porty SFP+ muszą umożliwiać ich obsadzanie wkładkami 10 Gigabit Ethernet – minimum 10GBase-SR, LR, oraz Gigabit Ethernet – minimum 1000Base- SX, 1000Base LX | TAK |  |
|  | **Parametry fizyczne:** Wysokość maksymalnie 1U, montowany w szafie typu rack 19’’ | TAK |  |
|  | **Pamięć**:* Co najmniej 512 MB SDRAM

Co najmniej 256 MB pamięci flashBufor pakietów co najmniej 1.5 MB | TAK |  |
|  | **Procesor**: min. CPU ARM Cortex-A9 @ 800 MHz | TAK |  |
|  | **Wielkość tablicy adresów MAC**: co najmniej 16000 | TAK |  |
|  | **Ilość obsługiwanych sieci VLAN**: co najmniej 256 | TAK |  |
|  | **Wydajność:** • Przepustowość przełączania: min. 128 Gbit/s • Przełączanie dla pakietów: min. 95.23 Mpps. • Opóźnienie:* < 4.7 uSec dla 100 Mb

< 2.4 uSec dla 1000 Mb<1.3 uSec dla 10 GbpsObsługa ramek Jumbo o wielkości co najmniej 9216 bajtów | TAK |  |
|  | **Funkcjonalność urządzenia:*** obsługa agregacji portów zgodnie z LACP (IEEE 802.3ad),

obsługa protokołu SNTP,Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), MSTP (802.1s)Minimum 256 obsługiwanych sieci VLANAutomatyczne przydzielanie klasy urządzenia PoE w oparciu o LLDP oraz LLDP-MED.Minimum 50 możliwych do utworzenia list ACL,CoS zgodna z 802.1pVoice VLANMinimum 509 wpisów ARPMożliwość przechowywania dwóch obrazów oprogramowania: aktywny i zapasowyPort SecurityDHCP SnoopingKlient RadiusPort mirroring,DHCP Relay,DoS Protection,ARP Attack Protection,Możliwość utworzenia minimum 32 statycznych wpisów w tablicy routingu | TAK |  |
|  | **Zasilanie**: zasilacz 230V AC wbudowany, | TAK |  |
|  | **Temperatura pracy:** 0°C do 40°C | TAK |  |
|  | **Maksymalny pobór mocy**: 460W | TAK |  |
|  | **Zarządzanie**: WWW (GUI), SNMP Manager, cloud-based web portal | TAK |  |
|  | **Gwarancja**: min. 5 lat | TAK |  |
|  | **Wykonawca winien przedłożyć dokumenty**:* Deklaracja zgodności CE oferowanego urządzenia – certyfikat potwierdzony za zgodność z oryginałem,

Oświadczenie producenta lub oświadczenie autoryzowanego przedstawiciela producenta potwierdzające zgodność wszystkich parametrów oferowanego urządzenia wskazanych w Opisie przedmiotu zamówienia. | TAK |  |

Zakup i dostawa oprogramowania typu NAC

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymaganie | Wymagane bezwzględnie | Spełnienie przez OferentaTAK/NIE |
|  | **Podstawowa funkcjonalność:**-System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.-System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor).-System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.-System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.-System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.-System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.-System musi umożliwiać obsługę co najmniej 250 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 50000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.-Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.-System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.-System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.xMaszyny fizyczne - serwery wspierane przez producenta.System musi posiadać funkcjonalność serwerów:serwera RADIUS dla infrastruktury sieciowej,serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,serwera VPN,serwera DNS,serwera SYSLOG,serwera TFTP,serwera TACACS+,serwera Monitoringu,serwera DHCP,serwera polityk uwierzytelniania i kontroli dostępu 802.1X,serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.-System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.-System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.-System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.-System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z innych systemów zewnętrznych.-Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, konfiguracji VPN, wysłania konfiguracji dostępowych poprzez email.-System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.-System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.-System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.-System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.-Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).-System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. tożsamość, MAC adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.-System musi zapewniać scentralizowane zarządzanie urządzeniami sieciowymi. Zarządzanie musi odbywać się bezagentowo, a w systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.-System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.-System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych i końcowych za pomocą min. protokołu SNMP.-Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu: VLANów, autoryzacji, statusu, opisu.-System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.-System musi zapewniać funkcjonalność wizualizacji konfiguracji podsieci IP oraz przypisania jej do jednostek.-System musi posiadać funkcję zintegrowanego serwera DHCP.-System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.-System musi wspierać funkcjonalność włączania i wyłączania podsieci IP, adresów IP bez konieczności usuwania ich z systemu.-System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.-System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP.-System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.-System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).-System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS.-Captive Portal musi umożliwiać obsługę instalacji agentów, dystrybucji certyfikatów użytkowników oraz generowania autokonfiguratorów sieci.-System musi posiadać mechanizm zarządzania uprawnieniami użytkowników, którzy będą mogli rejestrować swoje urządzenia, pobierać certyfikaty, agenty oraz uruchamiać autokonfiguratorów sieci.-Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.-Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.-Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.-Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).-Captive Portal powinien umożliwiać konfigurację maksymalnej ilości nieudanych logowań.-System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.-System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego, co najmniej:Palo AltoFortigateSophosFlowMonESET NOD32CheckPoint-System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.-System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.-System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.-System musi obsługiwać metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej: DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.-System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach:FortiGatePulse SecureOpenVPNPalo AltoCisco ASA-System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:Czy system jest aktualny z możliwością automatycznego naprawienia niezgodnościCzy włączony jest firewallCzy jest uruchomiony system antywirusowy i aktualna baza sygnaturCzy jest włączone szyfrowanie dysku systemowegoCzy urządzenie końcowe jest podłączone do domeny Microsoft Active DirectoryCzy na dysku znajdują się pliki lub katalogi wskazane przez administratoraCzy w systemie są uruchomione procesy wskazane przez administratoraCzy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodnościCzy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:Wartości klucza rejestruTypu wartości: Number, String, Version-System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.-System musi współpracować z serwerem tokenów.-System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej Microsoft Windows, Mac OS, iOS, Android.-System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).-System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.-System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą min. wiadomości e-mail, Syslog, notyfikacji systemowych.-System musi zapewniać wsparcie dla obsługi serwerów TACACS+. | TAK |  |
|  | **Mechanizmy uwierzytelnienia**-System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.-System musi obsługiwać uwierzytelnianie w oparciu o minimum następujące protokoły: MAC, PAP/ASCII, CHAP, SNMP, 802.1X wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), itp.-System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.-System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.-System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).-System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:Tożsamość/Urządzenie końcowe,Grupa tożsamości/urządzeń końcowych,Parametry urządzeń końcowych, min: system operacyjny, wersja,Atrybuty Active Directory,Jednostka organizacyjna tożsamości/urządzeń końcowych,Urządzenia sieciowe sieci przewodowej, bezprzewodowej,Grupy urządzeń sieciowych,Porty urządzeń sieciowych,Grupy portów urządzeń sieciowych,Jednostka organizacyjna portów,Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),Data, czas ważności polityki,Wewnętrzny Captive Portal,Metoda autoryzacji.-System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.-System musi posiadać lokalną bazę tożsamości, tworzone w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.-System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.-System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.-System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.-System musi pozwalać na weryfikację zalogowanego urządzenia końcowego IoT (Internet of Things) minimum za pomocą mechanizmów SNMP, DHCP, NMAP, Agenta oraz wywołania akcji: powiadomienie administratorów i/lub zablokowanie i rozłączenie sesji.-System musi wspierać funkcjonalność różnych typu autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.-System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.-System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP. | TAK |  |
|  | **Obsługa serwerów certyfikatów CA**-System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.-Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).usługę OCSP (Online Certificate Status Protocol). | TAK |  |
|  | **Obsługa serwerów VPN****-**System musi posiadać funkcję zintegrowanego serwera VPN oraz zapewniać współpracę z zintegrowanym oraz zewnętrznym serwerem CA,-System musi umożliwiać wystawianie konfiguracji klienckich, certyfikatów dla serwerów VPN.-System musi logować wszelkie próby autoryzacji do serwerów VPN.-System musi zapewniać przynajmniej następujące funkcjonalności serwera VPN:-Logowanie do zasobów firmy,-Obsługę OTP,-Przypisanie ustalonego adresu IP. | TAK |  |
|  | **Obsługa serwerów DNS****-**System musi posiadać funkcję zintegrowanego serwera DNS.-System musi umożliwiać graficzne zarządzanie serwerami DNS.-System musi zapewniać przynajmniej następujące funkcjonalności serwera DNS:-Zarządzanie strefami,-Zarządzanie rekordami stref,-Zatwierdzanie przez administratorów moderowanych rekordów stref,-Weryfikacja konfiguracji przed instalacją,-Instalacja konfiguracji na serwerach DNS. | TAK |  |
|  | **Obsługa serwerów DHCP****-**System musi posiadać funkcję zintegrowanego serwera DHCP.-System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.-System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:Uruchamianie usługi dla wybranych podsieci,Przypisanie ustalonego adresu IP dla adresu MAC.Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,Możliwość określania braku dostępu dla wybranych adresów MAC,Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,Dokonywanie zmian bez konieczności wyłączania usług. | TAK |  |
|  | **Obsługa serwerów TACACS+**-System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych.-System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.-System musi umożliwiać tworzenia haseł administratorom.-System musi umożliwiać tworzenie listy komend uprawnień dla administratorów-System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.-System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.-System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.-System musi wspierać logowanie administratorów za pomocą tokenów OTP. | TAK |  |
|  | **Raportowanie i monitoring**-System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:-Monitoring co najmniej: zdarzeń autoryzacji, zdarzeń systemowych, zdarzeń DHCP, tożsamości, urządzeń końcowych, urządzeń sieciowych.-Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.-Raport ze zdarzeń logowania z informacją o nadam adresie IP.-Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.-Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.-System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.-System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.-System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.-System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.-System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.-System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.-Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.-Raport zdarzeń Microsoft Active Directory, min. logowania i wylogowania z system (w tym błędne logowania), logowania do sieci 802.1X. |  |  |
|  | **Alarmy**-System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą min. wiadomości e-mail, Syslog, notyfikacji systemowych.-System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:- badanie łączności IP za pomocą ping, traceroute,- tcpdump protokołów RADIUS, TACACS+, - wyszukiwanie zdarzeń RADIUS z uwzględnieniem nazwy użytkownika,  adresu MAC, statusu uwierzytelnienia (udana lub nieudana), powodu,  jeżeli uwierzytelnienie nieudane, zakresu czasowego, co do dnia,  godziny i minuty, wykonanie zdalnego polecenia na urządzeniu  sieciowym |   |  |
|  | **Szkolenie administratorów**Certyfikowane szkolenie z ww. oprogramowania w miejscu producenta oprogramowania z terminem do końca roku 2022 dla 3 osób. Wykonawca zapewni przejazd, zakwaterowanie, wyżywienie na cały okres szkolenia | TAK |  |

Zakup i dostawa oprogramowania do monitorowania, zarządzania siecią i stacjami roboczymi

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymaganie | Wymagane bezwzględnie | Spełnienie przez OferentaTAK/NIE |
|  | **Moduł sieciowy**Lista wymaganych funkcji:* skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP

interaktywne mapy sieci, mapy użytkownika, oddziałów, mapy inteligentnejednoczesna praca wielu administratorów, zarządzanie uprawnieniami, dzienniki dostępuserwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.)liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp.możliwość nakładania na urządzenie liczników wydajności wg szablonu (wzorca)działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeńliczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne)kompilator plików MIBobsługa pułapek SNMProutery i switche: mapowanie portówobsługa komunikatów syslogalarmy zdarzenie - akcjapowiadomienia (pulpitowe, e-mail, SMS) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.)raporty (dla urządzenia, oddziału, wybranej mapy lub całej sieci) | TAK |  |
|  | **Moduł do inwentaryzacji**Lista wymaganych funkcji:* audyt inwentaryzacji sprzętu i oprogramowania

wgląd w licencje przypisane do użytkownika pracującego na wielu urządzeniachzdalny dostęp do managera plików z możliwością usuwania plików użytkownikainformacje o wpisach rejestrowych, plikach i archiwach .zip na stacji roboczejszczegółowe informacje o konfiguracji sprzętowej konkretnej stacji roboczejzarządzanie instalacjami/dezinstalacjami oprogramowania w oparciu o menedżera pakietów MSIalarmy: instalacja oprogramowania, zmiana w zasobach sprzętowychlista kluczy oprogramowania Microsoftaplikacja dla systemu Android umożliwiająca spis z natury na bazie kodów kreskowych, kodów QRmożliwość archiwizacji i porównywania audytówmonitorowanie harmonogramu zadań Windows | TAK |  |
|  | **Moduł do zarządzania użytkownikami**Lista wymaganych funkcji:* minimalizacja zjawiska cyberslackingu i zwiększenie wydajności pracowników

redukcja kosztów wydrukublokowanie stron WWWblokowanie uruchamianych aplikacjimonitorowanie wiadomości e-mail (nagłówki) - antyphishingszczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy)użytkowane aplikacje (aktywnie i nieaktywnie)odwiedzane strony WWW (tytuły i adresy stron, liczba i czas wizyt)audyty wydruków (drukarka, użytkownik, komputer), koszty wydrukówużycie łącza: generowany przez użytkowników ruch sieciowystatyczny zdalny podgląd pulpitu użytkownika (bez dostępu)zrzuty ekranowe (historia pracy użytkownika ekran po ekranie)blokowanie uruchamiania procesów na podstawie lokalizacji pliku .EXEzarządzanie regułami blokowania aplikacji i stron WWW (tworzenie, grupowanie, powielanie między grupami użytkowników) | TAK |  |
|  | **Moduł pomocy/wsparcia technicznego**Lista wymaganych funkcji:* rozbudowany system raportów

powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistymbaza zgłoszeń z rozbudowaną wyszukiwarkąbaza wiedzy z kategoryzacją artykułów i możliwością wstawiania grafik oraz filmów z YouTubeprzejrzysty i intuicyjny interfejs webowywewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowychkomunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytuzdalny dostęp do komputerów z możliwością blokady myszy/klawiaturydwukierunkowa wymiana plikówzarządzanie procesami Windows z poziomu okna informacji o urządzeniuzadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania)procesowanie zgłoszeń z wiadomości e-mailintegracja bazy użytkowników z Active Directoryzarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont). | TAK |  |
|  | **Moduł ochrony danych**Lista wymaganych funkcji:* zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami

informacje o urządzeniach podłączonych do danego komputeralista wszystkich urządzeń podłączonych do komputerów w sieciaudyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowychzarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkownikówcentralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directoryintegracja bazy użytkowników i grup z Active Directoryalarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym | TAK |  |
|  | **Moduł administracyjny**Lista wymaganych funkcji:* Network: liczniki wydajności, alarmy oraz odpowiedzi serwisów TCP/IP

Inventory: zmiany w konfiguracji sprzętowej urządzeń, zmiany w konfiguracji aplikacyjnej urządzeń, alarmy dla zasobówUsers: statystyki wydruków, dane z używanych oraz uruchomionych aplikacji, wysycenie łącz, aktywność na stronach WWWHelpDesk: statystyki z obsługi zgłoszeń, lista najnowszych oraz najstarszych nierozwiązanych zgłoszeń, metryki SLA dla zgłoszeńDataGuard: ostatnie podłączane nośniki zewnętrzne, ostatnie operacje na plik | TAK |  |

Zakup i dostawa sprzętu komputerowego

1. Zestaw komputerowy

a) stacja administratora do zarządzania, monitorowania sieci (2sz.)

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymaganie | Wymagane bezwzględnie | Spełnienie przez OferentaTAK/NIE |
|  | **Procesor**: Min. 6-rdzeniowy, osiągający w zaoferowanej konfiguracji w teście PassMark CPU Mark wynik min. 17500 punktów. Do oferty należy dołączyć wydruk ze strony: http://www.cpubenchmark.net potwierdzający spełnienie wymogów SIWZ | TAK |  |
|  | **Pamięć RAM**: 1 x 16GB 2666 MHz możliwość rozbudowy do min 64GB, minimum 1 slot wolny na dalszą rozbudowę | TAK |  |
|  | **Parametry pamieci masowej:** Min. 480 GB SSD NVMe | TAK |  |
|  | **Karta graficzna**: Zintegrowana z płytą główną, ze wsparciem dla DirectX 12.1, OpenGL 4.5, Open CL 1.2 oraz dla rozdzielczości 3840x2160@60Hz osiągająca w teście Average G3D Mark wynik na poziomie 1540 punktów. | TAK |  |
|  | **Obudowa:**Typu Desktop Mini z możliwością pracy w pozycji pionowej i poziomej, o maksymalnej sumie wymiarów 387 mm posiadająca min.: min 1 wewnętrzną półkę dla 1 szt dysku 2,5”. Zaprojektowana i wykonana przez producenta komputera opatrzona trwałym logo producenta, metalowa. Obudowa musi umożliwiać serwisowanie komputera bez użycia narzędzi (m.in.: wymiana pamięci RAM) oraz dawać możliwość instalacji dysku twardego M.2 PCIe. Otwarcie obudowy zabezpieczone śrubą serwisową, którą można odkręcić bez użycia narzędzi.Z przodu obudowy wymagany jest wbudowany fabrycznie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, który musi sygnalizować co najmniej:-awarie procesora -awarie BIOS-uszkodzenie kontrolera Video-uszkodzenie pamięci RAM-uszkodzenie zasilania-przegrzanie procesoraObudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady typu Kensingtona) oraz kłódki (oczko na kłódkę)Zasilacz zewnętrzny o mocy max 65W i sprawności min 89% dla 100% użycia | TAK |  |
|  | **BIOS- Możliwość odczytania z BIOS:** 1. Wersji BIOS wraz z datą wydania wersji2. Modelu procesora, prędkości procesora, wielkość pamięci cache L1/L2/L33. Informacji o ilości pamięci RAM wraz z informacją o jej prędkości, pojemności i obsadzeniu na poszczególnych slotach 4. Informacji o dysku twardym: model, pojemność, 5. Informacji o MAC adresie karty sieciowej6. Zaimplementowany w BIOS podstawowy system diagnostyczny umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych. Minimalne funkcjonalności systemu diagnostycznego:- test procesora- test pamięci RAM- test dysku twardego- test płyty głównejMożliwość wyłączenia/włączenia: zintegrowanej karty sieciowej, kontrolera audio, serial portu, portów USB (przód, tył), funkcjonalności ładowania zewnętrznych urządzeń przez port USB, slotu SATA, wewnętrznego głośnika, funkcji TurboBoost, wirtualizacji z poziomu BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.BIOS musi posiadać funkcję update BIOS z opcją automatycznego update BIOS przez sieć włączaną na poziomie BIOS przez użytkownika bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. | TAK |  |
|  | **Certyfikaty i standardy:*** Certyfikat ISO 9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)
* Deklaracja zgodności CE (załączyć do oferty)
* Komputer musi spełniać wymogi normy EPEAT 2019 na poziomie min GOLD dla Polski
* Komputer musi spełniać wymogi TCO Certified Desktops 8
 | TAK |  |
|  | **Warunki gwarancji:**- 36 miesięczna gwarancja producenta.- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.- Oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.- Wsparcie techniczne producenta Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera (ogólnopolski numer – w ofercie należy podać numer telefonu) dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia:- weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć)- czasu obowiązywania i typ udzielonej gwarancji | TAK |  |
|  | **Wymagania dodatkowe:**1. Zainstalowany system operacyjny Windows 10 Professional 64bit PL nie wymagający aktywacji za pomocą telefonu lub Internetu2. Wbudowane porty i złącza:- porty wideo: min. 1 szt HDMI 1.4 i 1 szt Display Port 1.4 z Dual-Mode (DP++)- Flex Port 1 - 1 szt portu do wyboru na poziomie produkcji tj.: Display Port 1.4 lub HDMI 2.0 lub VGA lub USB typ-C ze wsparciem dla Display Port i Power Delivery do 100W lub Serial port (RS232) - min. 7 szt USB w tym: 3 porty USB z przodu: - 1 szt UCB 3.2 Gen 2 typ-C z ładowaniem zewnętrznych urządzeń do 5V/3A, - 1 szt USB 3.2 Gen 1 typ-A z ładowaniem zewnętrznych urządzeń do 5V/1.5A, - 1 szt USB 3.2 Gen 2 typ-A4 porty USB typ-A z tyłu obudowy- Flex Port 2 – do wyboru: 2 x USB 2.0 typ-A lub Serial (RS-232)- port sieciowy RJ-45, - porty audio: z przodu obudowy port audio COMBO Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp..3. Karta sieciowa 10/100/1000 Ethernet RJ 45 (zintegrowana) z obsługą PXE, WoL, vPRO + karta WiFi 6 AX 2x2 z Bluetooth M.2 Combo Card vPro4. Płyta główna z chipsetem min Q470, wyposażona w:- 2 złącza DIMM z obsługą do 64GB pamięci RAM 2666MHz DDR4- 1 złącze M.2 PCIe x1 dla modułu WiFi- 1 złącze M.2 PCIe x1 dla dysku SSD- 1 złącze SATA dla dysku 2,5” | TAK |  |
|  | **Klawiatura USB w układzie polski programisty** | TAK |  |
|  | **Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll)** | TAK |  |
|  | **Nagrywarka SATA DVD +/-RW x8 – zewnętrzna** | TAK |  |

b) Monitor (4 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymaganie | Wymagane bezwzględnie | Spełnienie przez OferentaTAK/NIE |
|  | **Przekątna ekranu**: 27" | TAK |  |
|  | **Typ panela**: IPS | TAK |  |
|  | **Współczynnik kształtu**: 16:9 | TAK |  |
|  | **Rozdzielczość**: min. 3840 x 2160 | TAK |  |
|  | **Interfejsy**: DisplayPort, HDMI, VGA | TAK |  |
|  | **Standard VESA**:100x100 | TAK |  |
|  | **Wbudowane głośniki**  | TAK |  |
|  | **Gwarancja**: 36 miesięcy (w miejscu instalacji) | TAK |  |

2. Dysk HDD (16 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymaganie | Wymagane bezwzględnie | Spełnienie przez OferentaTAK/NIE |
|  | **Minimalne wymagania:** | TAK |  |
|  | **Pojemność**: min. 6TB | TAK |  |
|  | **Interfejs**: SATA 6GB (SATA III) | TAK |  |
|  | **MTBF:** min. 1mln | TAK |  |
|  | **Klasa dysku**: Enterprise/NAS Drives | TAK |  |
|  | Produkt musi być kompatybilny z QNAP TVS-871U-RP (lista zgodności dostępna na stornie: [https://www.qnap.com/pl-pl/compatibility)/](https://www.qnap.com/pl-pl/compatibility%29/) W razie uszkodzenia/awarii dysk zostaje u zamawiającego. | TAK |  |

.................................., dnia : .............................