**OPIS PRZEDMIOTU ZAMÓWIENIA**

Modernizacja infrastruktury informatycznej obejmuje:

1. System Bezpieczeństwa – klaster 2 urządzeń.

2. Przełącznik sieciowy PoE – 1szt.

3. Przełącznik sieciowy LAN – 4szt.

4. System komunikacji VoIP - 1 szt.

5. Aparat telefoniczny typ 1 - 15szt.

6. Aparat telefoniczny typ 1 - 1szt.

7. Warstwa wirtualizacji – 1 szt.

8. System kopii zapasowych – 1 szt.

9. SERWER - 2 szt.

10. WinSvrDCCore 2019 Sngl OLP 16 lic.

11. Serwer CAL 2019 Sngl Academic OLP 150 lic.

## **System Bezpieczeństwa – klaster 2 urządzeń.**

# **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 10 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

# **Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.

# **Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:

* 10 portami Gigabit Ethernet RJ-45.

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 realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 128 GB.
4. System musi być wyposażony w zasilanie AC.

# **Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 700 tyś. jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 6 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,8 Gbps.
4. Wydajność szyfrowania IPSec VPN: nie mniej niż 6 Gbps.
5. 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 1,4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 630 Mbps.

# **Funkcje Systemu Bezpieczeństwa:**

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.

# **Polityki, Firewall**

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory 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.

1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

# **Połączenia VPN**

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

* Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19 i 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

# **Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

* Routingu statycznego.
* Policy Based Routingu.
* Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

1. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

# **Zarządzanie pasmem**

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

# **Kontrola Antywirusowa**

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

# **Ochrona przed atakami**

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. 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.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

# **Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

# **Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

# **Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

# **Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

# **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.
2. 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.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

# **Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.
* ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
* ICSA dla funkcji SSL VPN.

# **Serwisy i licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

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 [x] miesięcy.

# **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.

## **Przełącznik sieciowy PoE – 1szt.**

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, w której wymagane mechanizmy centralnego systemu bezpieczeństwa obejmują elementy warstwy dostępowej sieci, wymaganym jest dostarczenie przełącznika współpracującego z oferowanym systemem bezpieczeństwa, w zakresie opisanym w sekcjach: "Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC" oraz "Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa", o następujących parametrach:

# **Parametry fizyczne platformy**

* Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
* Zasilanie AC 230V.
* Budżet mocy dla portów PoE min.: 370 W.
* Maksymalny pobór mocy: 400 W.
* Minimalny zakres temperatury pracy: 0-40ᵒC.

# **Interfejsy sieciowe - wymagania minimalne**

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 24 porty GE, RJ-45.

* W tym porty PoE w ilości co najmniej: 24, zgodne ze standardem: 802.3af oraz 802.3at.

b) 4 porty GE, SFP.

# **Zarządzanie**

* Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
* Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
* Wsparcie dla SNMP w wersjach 1-3.
* Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
* Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
* Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
* Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
* Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
* Funkcja definiowania ról administratorów przydzialających tryb dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
* Automatycznie wykonywane rewizje konfiguracji.

# **Parametry wydajnościowe**

* Przepustowość urządzenia - min. 56 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 40 Mpps.
* Tablica adresów MAC o pojemności co najmniej 8 k wpisów.
* Opóźnienie wprowadzane przez przełącznik - poniżej 4 mikrosekund.

# **Wymagane funkcje**

* Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
* Obsługa Jumbo Frames.
* Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
* Agregacja portów zgodna ze standardem 802.3ad.
* Obsługa co najmniej 4000 VLANów, zgodna ze standardem 802.1Q.
* Wsparcie dla Private VLAN.
* Port-mirroring.
* Uwierzytelinanie 802.1x na poziomie portu.
* Uwierzytelinanie 802.1x w oparciu o adres MAC.
* W ramach 802.1x wsparcie dla dedzkowanego VLANu dla gości (guest VLAN).
* W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
* W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.

# **Dodatkowe funkcje urządzenia przy integracji z sytemem centralnego zarządzania / NAC**

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

* Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
* Centralne zarządzanie sieciami VLAN.
* Rozpoznawanie urządzeń uzyskujących dostęp do sieci.
* Obsługa białych i czarnych list adresów MAC.
* Wykrywanie aplikacji komunikujących się w sieci.
* Musi być możliwe redundantne połączenie z elementami zarządzającymi.

# **Funkcje urządzenia przy integracji z sytemem centralnego zarządzania lub bezpieczeństwa**

* Stateful firewall, umożliwiający kontrolę pomiędzy sieciami VLAN.
* Routing statyczny i dynamiczny (co najmniej OSPF).
* Policy Based Routing.

# **Gwarancja oraz wsparcie**

1. 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.

## **Przełącznik sieciowy LAN – 4szt.**

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, w której wymagane mechanizmy centralnego systemu bezpieczeństwa obejmują elementy warstwy dostępowej sieci, wymaganym jest dostarczenie przełącznika współpracującego z oferowanym systemem bezpieczeństwa, w zakresie opisanym w sekcjach: "Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC" oraz "Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa", o następujących parametrach:

# **Parametry fizyczne platformy**

* Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
* Zasilanie AC 230V.
* Wbudowany redundantny zasilacz.
* Maksymalny pobór mocy: 20 W.
* Minimalny zakres temperatury pracy: 0-50ᵒC.

# **Interfejsy sieciowe - wymagania minimalne**

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 24 porty GE, RJ-45.

b) 4 porty GE, SFP.

# **Zarządzanie**

* Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania.
* Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
* Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
* Wsparcie dla SNMP w wersjach 1-3.
* Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
* Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
* Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
* Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
* Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
* Funkcja definiowania ról administratorów przydzialających tryb dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
* Automatycznie wykonywane rewizije konfiguracji.

# **Parametry wydajnościowe**

* Przepustowość urządzenia - min. 56 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 82 Mpps.
* Tablica adresów MAC o pojemności co najmniej 16 k wpisów.
* Opóźnienie wprowadzane przez przełącznik - poniżej 1 mikrosekund.

# **Wymagane funkcje**

* Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
* Obsługa Jumbo Frames.
* Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
* Agregacja portów zgodna ze standardem 802.3ad.
* Obsługa co najmniej 4000 VLANów, zgodna ze standardem 802.1Q.
* Wsparcie dla Private VLAN.
* Obsługa routingu statycznego.
* Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP.
* Port-mirroring.
* Uwierzytelinanie 802.1x na poziomie portu.
* Uwierzytelinanie 802.1x w oparciu o adres MAC.
* W ramach 802.1x wsparcie dla dedzkowanego VLANu dla gości (guest VLAN).
* W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
* W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
* Obsługa protokołu sFlow.

# **Dodatkowe funkcje urządzenia przy integracji z sytemem centralnego zarządzania / NAC**

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

* Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
* Centralne zarządzanie sieciami VLAN.
* Rozpoznawanie urządzeń uzyskujących dostęp do sieci.
* Obsługa białych i czarnych list adresów MAC.
* Wykrywanie aplikacji komunikujących się w sieci.
* Musi być możliwe redundantne połączenie z elementami zarządzającymi.

# **Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa**

* Stateful firewall, umożliwiający kontrolę pomiędzy sieciami VLAN.
* Routing statyczny i dynamiczny (co najmniej OSPF).
* Policy Based Routing.

# **Gwarancja oraz wsparcie**

1. 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.

## **System komunikacji VoIP - 1 szt.**

W ramach postępowania wymaganym jest dostarczenie centralnego systemu komunikacji VoIP, umożliwiającego centralizację procesu rejestrowania aparatów, zarządzania połączeniami telefonicznymi oraz kontami użytkowników.

Rozwiązanie musi zostać dostarczone w postaci dedykowanej platformy sprzętowej. Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa.

## Parametry fizyczne:

1. Nie mniej niż 2 porty 10/100 base-T.
2. Nie mniej niż 6 portów FXO.
3. Nie mniej niż 2 porty FXS.
4. Powierzchnia dyskowa - minimum 8 GB.

## Funkcje PBX:

W ramach systemu telefonii VoIP muszą być realizowane, co najmniej poniższe funkcje:

1. Konfigurowalna konsola recepcjonisty (Auto attendant / IVR) – funkcjonalność zapewniająca automatyczne odebranie połączenia na wypadek niedostępności recepcjonisty wraz z odtworzeniem nagranych wiadomości powitalnych.
2. Voicemail – poczta głosowa.
3. Voicemail to e-mail – powiadomienie poprzez e-mail o nagranej wiadomości na poczcie głosowej.
4. Conference – połączenia konferencyjne.
5. Ring Group – połączenia grupowe.
6. Dial-by-name directory – wybieranie połączenia po nazwie użytkownika.
7. Call Park – możliwość zawieszenia połączenia.
8. Music on hold – odtwarzanie muzyki podczas połączeń oczekujących.
9. Call cascade/Follow me – możliwość zestawiania połączeń kaskadowych.
10. Extension groups – możliwość tworzenia grup rozszerzonych na potrzeby np. przekierowania połączenia.
11. System Speed Dial – szybkie wybieranie numerów.
12. Fax over IP – przesyłanie fax’ów przez sieć IP.
13. Fax to e-mail – przesyłanie fax’ów na skrzynkę pocztową e-mail.
14. Fax Archive – archiwum fax’ów.
15. Paging – przywoływanie.
16. Hot Desking – możliwość zalogowania użytkownika na innym aparacie.
17. Operator Console – konsola operatorska.
18. Line Appearance (BLF) – możliwość monitorowania poszczególnych linii / numerów telefonicznych.
19. Extension Appearance (BLF) - możliwość monitorowania poszczególnych grup rozszerzeń.
20. Call queing – kolejkowanie połączeń.
21. Call/Contact Center – wbudowana funkcjonalność contact center.
22. Hotel Management – możliwość integracji z systemami PMS.

## Obsługiwane Standardy Voice/Video/QoS

W ramach systemu telefonii VoIP muszą być realizowane, co najmniej poniższe funkcje:

1. Obsługiwane kodeki głosu: G.711U-law, G.711A-law, G.729, G.722, G.726, GSM
2. Obsługiwane kodeki video: H.263, H.264
3. Wsparcie dla Fax’u: T.38
4. L2 QoS: 802.1p/Q voice tagging
5. L3 QoS: Diffserv voice tagging

## Wsparcie dla następujących protokołów:

W ramach systemu telefonii VoIP muszą być realizowane, co najmniej poniższe funkcje:

1. Wsparcie dla SIP (RFC 3261).
2. Wsparcie dla następujących kodeków głosu:   G.711U-law, G.711A-law, G.729a, G.722, G.726, GSM.
3. Wsparcie dla następujących kodeków wideo: H.263, H.264.
4. SIP transport: UDP oraz TCP.
5. Szyfrowanie SIP: SIP over TLS - TLS 1.0.
6. Szyfrowanie mediów: SRTP.
7. Dostęp administracyjny:   HTTP, HTTPS, SSH.
8. Session Description Protocol (SDP).
9. Wsparcie dla IPv6.
10. Wsparcie dla SNMP  v1, v2 oraz v3.
11. Wsparcie dla NTP/SNTP.
12. DTMF: RFC 2833, Inband, SIP Info.
13. Wsparcie dla SIP UPDATE method  (RFC 3311).

## Funkcje zarządzania:

1. Konfiguracja za pomocą interfejsu graficznego (GUI) oraz linii komend (CLI).
2. Zarządzanie kontami / uprawnieniami użytkowników systemu.
3. Wsparcie dla uwierzytelniania w oparciu o usługi katalogowe (LDAP).
4. Funkcjonalność „network traffic capture” – możliwość przechwycenia i zapisu ruchu sieciowego (Wireshark).
5. Funkcjonalność CDR (Call Detail Recording).
6. Automatyczna konfiguracja aparatów – poprzez mDNS oraz DHCP opcja 66.

## Wsparcie dla zewnętrznych systemów:

1. Współpraca z systemami takimi jak PMS, SDMR.

## Wymagane licencje:

1. System komunikacji VoIP musi umożliwiać podłączenie do 50 aparatów telefonicznych.
2. Jeżeli system komunikacji VoIP tego wymaga, konieczne jest dostarczenie licencji do obsługi / przyłączenia 50 aparatów telefonicznych.

## 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.

## **Aparaty telefoniczne:**

Wraz z systemem wymagane jest dostarczenie kompatybilnych fizycznych aparatów telefonicznych pochodzących od tego samego producenta co system telefoniczny. Aparaty muszą spełniać następujące parametry:

## **Aparat telefoniczny typ 1 - 15szt.**

* 1. Wsparcie dla SIP (RFC 3261).
  2. Wsparcie dla kodeków: G.711 µ-law/a-law, G.729a.
  3. Kolorowy, podświetlany wyświetlacz o przekątnej ekranu - minimum 2.4 cali.
  4. Programowalne fizyczne przyciski funkcyjne – minimum 4.
  5. Fizyczne dedykowane przyciski funkcyjne – minimum 5.
  6. Wbudowana książka telefoniczna – minimum 500 wpisów.
  7. Dioda powiadamiająca o nieodebranych połączeniach.
  8. Rejestr połączeń (nieodebrane/odebrane/wychodzące)- minimum 100.
  9. Możliwość zasilania telefonu poprzez PoE 802.3af.
  10. Dwa port Ethernet RJ-45 10/100.
  11. Wsparcie dla zewnętrznych zestawów nagłownych (RJ-22) wraz z dedykowanym przyciskiem do przełączenia pomiędzy zestawem słuchawkowym a nagłownym.
  12. Wbudowany system głośnomówiący (full-duplex).
  13. Możliwość automatycznego wykrycia telefonu przez system telefoniczny poprzez sieć LAN.

## **Aparat telefoniczny typ 1 - 1szt.**

1. Wsparcie dla SIP (RFC 3261).
2. Wsparcie dla kodeków: G.711 µ-law/a-law, G.729a.
3. Kolorowy, podświetlany wyświetlacz o przekątnej ekranu - minimum 4.3 cali.
4. Programowalne fizyczne przyciski funkcyjne – minimum 4.
5. Fizyczne dedykowane przyciski funkcyjne – minimum 11.
6. Wbudowana książka telefoniczna – minimum 1000 wpisów.
7. Dioda powiadamiająca o nieodebranych połączeniach.
8. Rejestr połączeń (nieodebrane/odebrane/wychodzące) - minimum 300.
9. Możliwość zasilania telefonu poprzez PoE 802.3af.
10. Dwa port Ethernet RJ-45 10/100/1000.
11. Wsparcie dla zewnętrznych zestawów nagłownych (RJ-22) wraz z dedykowanym przyciskiem do przełączenia pomiędzy zestawem słuchawkowym a nagłownym.
12. Wbudowany system głośnomówiący (full-duplex).
13. Możliwość automatycznego wykrycia telefonu przez system telefoniczny poprzez sieć LAN.

## **Warstwa wirtualizacji - 1 szt.**

Oferowana równoważna warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym, nie może być częścią innego systemu operacyjnego oraz musi spełniać poniższe warunki:

1. Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego.
2. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12TB pamięci fizycznej RAM.
3. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.
4. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB.
7. Rozwiązanie musi wspierać następujące systemy operacyjne: MS-DOS 6.22, Windows XP, Windows Vista, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows 7, Windows 8, SLES 12, SLES 11, SLES 10, SLES 9, SLES 8, REHL 7, RHEL 6, RHEL 5, RHEL 4, RHEL 3, RHEL Atomic 7, Solaris 11 ,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X, Photon OS, eCommStation 1/2/2.1, Oracle Linux , CoreOS, NeoKylin.
8. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
9. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych.
10. Rozwiązanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Windows 7, a także instalacji wszystkich funkcjonalności w tym Hyper-V pakietu Windows Server 2012 na maszynie wirtualnej.
11. Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
12. Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.
13. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
14. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
15. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP.
16. Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
17. System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.
18. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
19. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
20. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
21. Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
22. Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.
23. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
24. Rozwiązanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych.
25. Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.
26. Rozwiązanie replikujące musi gwarantować współczynnik RPO na poziomie nie większym 5 minut.
27. Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług.
28. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi oraz różnymi konsolami do zarządzania wirtualizacją. Rozwiązanie musi posiadać natywne mechanizmy szyfrowania, podczas przenoszenia maszyn wirtualnych, w czasie ich pracy pomiędzy serwerami fizycznymi.
29. Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury.
30. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych.
31. Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.
32. Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jaki zmianę jej wersji bez potrzeby wyłączania wirtualnych maszyn.
33. Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
34. Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana.
35. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
36. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.
37. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
38. Rozwiązanie musi umożliwiać konfiguracje HA dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu.
39. Oprogramowanie do wirtualizacji musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja) oraz wirtualizacji sieci (SDN) na wszystkich poziomach wsparcia (L1-L3). Wsparcie musi odbywać się poprzez jednorodny kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www pozwalający zarządzać licencjami i zgłaszać zlecenia serwisowe).
40. System musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader.
41. Wirtualizator musi wspierać TPM 2.0 oznacza to min. że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny uruchomił się z włączoną opcją „Secure Boot”. Po potwierdzeniu, że Secure Boot jest włączone,  system gwarantuje, że wirtualizator  uruchomił w prawidłowej, niezmienionej formie poprzez  weryfikację podpisu cyfrowego

Wirtualizator musi mieć włączenia funkcji  “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Windows 10 oraz Windows Server 2016.

1. System musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych.
2. Wirtualizator musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych Windows 10 oraz Windows 2016. Oznacza to, że punktu widzenia maszyny wirtualnej z systemem operacyjnym Windows 10 lub Windows 2016 wirtualny TPM widziany jest jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM przechowywana jest w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana. W związku z tym wszystkie standardowe funkcjonalności wirtualizatora tj. wysoka dostępność, czy przenoszenie maszyn wirtualnych bez ich wyłączania pomiędzy różnymi serwerami fizycznymi działa prawidłowo. Wirtualizator musi posiadać rolę administratora odpowiedzialnego za zarządzanie kluczami szyfrującymi. Rola ta powinna być odseparowana od roli administratora wirtualizatora. Oznacza, to, że tylko administrator odpowiedziany za szyfrowanie ma dostęp do kluczy szyfrujących oraz może zarządzać procesem szyfrowania w obrębie wirtualizatora.
3. Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich dostarczonych w ramach postępowania serwerów.
4. Rozwiązanie musi posiadać wsparcie dla natywnych dysków 4K.
5. Rozwiązanie wirtualizatora musi posiadać mechanizmy proaktywnej wysokiej dostępności. Oznacza, to, że jeśli serwer fizyczny posiada funkcję przekazania do wirtualizatora informacji o stanie serwera, to wirtualizatora na podstawie tych danych, wirtualizator jest w stanie, proaktywnie przenieść wszystkie maszyny wirtualne na inne prawidłowo działające serwery fizyczne w klastrze, zanim dojdzie do całkowitej awarii serwera fizycznego.

Licencje dostępne w modelu licencjonowania na procesor fizyczny (nielimitowana liczba rdzeni procesora).

Wymaga się dostarczenia licencji na 6 procesorów wraz z 3 letnim wsparciem i subskrypcją i trybem obsługi zgłoszeń 9 godzin przez 5 dni w tygodniu.

## **System kopii zapasowych .**

System spełniający poniższe wymagania:

1. System backupu powinien wspierać następujące systemy operacyjne: Windows, Linux, BSD, Mac OS, Novell, Solaris i Unix.
2. System backupu powinien umożliwić backup i odtworzenie (na pierwotnym lub innym hoście) całych maszyn wirtualnych zlokalizowanych na systemie wirtualizacji.
3. System powinien umożliwić odzyskiwanie poszczególnych plików maszyny wirtualnej i jej dysków wirtualnych.
4. System powinien umożliwić automatyczne testowanie i weryfikowanie każdej kopii zapasowej maszyny wirtualnej pod kątem możliwości odzyskania danych przez uruchomienie maszyny bezpośrednio z pliku kopii zapasowej (nie jest wymagane pełne przywrócenie maszyny), łącznie z obsługą niestandardowych skryptów do testowania aplikacji.
5. System powinien umożliwić wykluczanie wybranych plików i folderów z tworzenia kopii zapasowych i replikacji, ograniczając ilość danych wymagających przesłania i przechowywania.
6. W celu oszczędności czasu i pamięci masowej system powinien umożliwiać działanie w ciągłym trybie przyrostowym bez konieczności okresowego tworzenia pełnych kopii.
7. Obsługa baz danych Oracle i Microsoft SQL. System powinien umożliwić bezagentowe tworzenie kopii zapasowych dzienników transakcji, zarządzanie zarchiwizowanymi dziennikami i odzyskiwanie baz danych na poziomie transakcji na pierwotny lub nowy serwer.
8. System powinien umożliwić wyszukiwanie i przywracanie wszystkich rodzajów obiektów Active Directory (AD), w tym użytkowników, grup, kont komputerów i kontaktów oraz haseł użytkowników i komputerów.
9. System powinien umożliwić szybkie przywracanie usług przez uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej w zwykłej pamięci masowej.
10. System powinien posiadać portal odzyskiwania plików i maszyn wirtualnych dla operatorów działu wsparcia.
11. Oferowany system backupu powinien umożliwić realizację funkcji backupu maszyn wirtualnych z dowolnego hosta z klastra HA. Każdy host powinien mieć zapewnioną dożywotnią licencje na system backupu.
12. Wymagane jest wsparcie producenta dla systemu backupu. W ramach wsparcia musi być możliwość ściągania i instalacji update, upgrade oraz zgłaszania problemów do producenta za pomocą portalu web i/lub telefonu.

Wraz z systemem należy dostarczyć przestrzeń dyskową typu NAS służącą do przechowywania utworzonych kopii zapasowych spełniającą poniższe wymagania:

* Minimalna ilość zatok dyskowych 3,5 cala – 12 szt.
* Zamontowane dyski twarde: min 6x6TB
* Minimalna pamięć 4GB
* Ilość portów Ethernet: min 2 x 1GbE
* Obsługiwane mechanizmy RAID: Min. RAID5,RAID6
* Obsługiwane protokoły dostępowe: min. iSCSI, NFS

13. System musi być zalicencjonowany na wszystkie dostarczone serwery.

## **Serwer 2szt.**

|  |  |  |  |
| --- | --- | --- | --- |
| **LP** | **Parametr lub warunek** | | **Minimalne wymagania** |
| 1 | Obudowa | | -Typu Rack, wysokość maksimum 1U;  -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack oraz ramieniem porządkującym ułożenie przewodów w szafie rack; |
| 2 | Płyta główna | | -Dwuprocesorowa, wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów dwunastordzeniowych;  -wyposażona w minimum 24 gniazda pamięci RAM DDR4, obsługa minimum 3000GB pamięci RAM DDR4 2966 Mhz;  -Oferowany model serwera musi obsługiwać pamięć nieulotną instalowaną w gniazdach pamięci RAM o pojemności sumarycznej minimum 1000GB (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci)  -Minimum 3 złącza PCI Express generacji 3 o prędkości x16 (nie wliczając ewentualnego złącza dedykowanego dla kontrolera RAID;  -Wszystkie złącza PCI Express muszą być aktywne;  -Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slocie M.2 bez zajmowania klatek dyskowych serwera);  -Zainstalowany w dedykowanym slocie dysk SSD M.2 o pojemności minimum = 120GB i DWPD minimum = 1,5 wraz z fabrycznie preinstalowanym Vmware ESXi; |
| 3 | Procesory | | Zainstalowane minimum dwa procesory ośmio-rdzeniowe w architekturze x86 osiągające w oferowanym serwerze w testach wydajności [SPECrate2017\_int\_base](http://www.spec.org/auto/cpu2017/Docs/result-fields.html#SPECrate2017intbase) minimum 43 pkt. Baseline. Wynik dla oferowanego serwera wraz z oferowanymi procesorami dostępny na stronie spec.org; (nie dopuszcza się procesorów o innej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowana aplikacji i systemów operacyjnych) |
| 4 | Pamięć RAM | | -Zainstalowane 512 GB pamięci RAM typu DDR4 Registered, 2933Mhz w kościach o pojemności 32GB;  -Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC;  -Wsparcie dla konfiguracji pamięci w trybie „Rank Sparing” |
| 5 | Kontrolery dyskowe, I/O | | -Zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,50,60 2GB pamięci podręcznej cache,  -Wyposażony w nieulotną pamięć cache; |
| 6 | Dyski twarde | | -Zainstalowane 2 dyski SSD minimum 480GB SATA o parametrze DWPD minimum 3, dyski hotplug;  -Minimum 8 wnęk dla dysków twardych Hotplug 2,5; |
| 7 | Inne napędy zintegrowane | | Wbudowany fabrycznie wewnętrzny napęd Blue-ray (odczyt/zapis) / DVD-RW; |
| 8 | Kontrolery LAN | | -Jedna dwuportowa karta 2x1Gbit/s ze wsparciem iSCSI, niezajmująca slotu PCI Express;  -Dodatkowa osobna karta 2x 10Gbit/s SFP+, niezajmująca slotu PCI Express (dopuszcza się instalację w slocie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilości slotów PCI Express) |
| 9 | Kontrolery I/O FC/SAS/Inne | | -Jedna dwuportowa karta FC x16 chipset QLE2692; |
| 10 | Porty | | -zintegrowana karta graficzna ze złączem VGA;  -2x USB 3.0 dostępne na froncie obudowy  -2x USB 3.0 dostępne z tyłu serwera  -1x USB 3.0 wewnątrz serwera  -dodatkowe złącze VGA dostępne z przodu serwera;  Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera; |
| 11 | | Zasilanie, chłodzenie | Do podtrzymania zasilania w przypadku przerwy w dostawie energii do serwera musi być wmontowany (lub dostarczony jako osobna jednostka montowana w szafie RACK o wysokości nie większej niż 2U) zasilacz awaryjny (UPS) o następujących parametrach minimalnych:   * Moc znamionowa: min 2200 VA * Gniazdo wejściowe: C20 * Gniazda wyjściowe: min 8xC13, 1xC19 * W przypadku urządzenia zewnętrznego niezbędne jest aby posiadało ono kartę sieciową umożliwiającą zarządzanie zasilaczem * Napięcia wyjściowe: 230 V (+6/-10 %) * Częstotliwość wyjściowa: 50/60 Hz +/- 0,1 % * Poziom hałasu: < 45 dBA * Temperatura pracy: min. Od 0 do 40°C * Spełniane Normy: IEC/EN 62040-1-1 (Bezpieczeństwo), IEC/EN 62040-2 (EMC), IEC/EN 62040-3 (Charakterystyka)   -Redundantne zasilacze hotplug o mocy maksimum 450W, o sprawności 94% (tzw klasa Platinum)  -Redundantne wentylatory hotplug; |
| 12 | | Zarządzanie | Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system przewidywania, rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w slocie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zrządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera,  -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 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; * Dostęp poprzez przeglądarkę Web (także SSL, 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) * Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) * 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 itd.). * Dedykowana, wbudowana w kartę zarządzającą pamięć flash o pojemności minimum 16 GB * Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB); * Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania; * Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; * 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 (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji; * Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń); * Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą; * karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego w systemie producenta serwera). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera; |
| 13 | | Wspierane OS | - Windows 2016 Hyper-V, Windows 2012 R2 Hyper-V, VMWare, Suse, RHEL |
| 14 | | Gwarancja | 3 lata gwarancji producenta serwera w trybie onsite z gwarantowanym czasem skutecznej naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD Fixtime);  -Dostępność części zamiennych przez 5 lat od momentu zakupu serwera;  -Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji; |
| 15 | | 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 producenta serwera potwierdzające spełnienie wymagań dołączone do oferty).  -Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg;  -Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu;  -Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: 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; |

## **10. Licencja oprogramowania systemu operacyjnego Microsoft Windows Server 2019 Datacenter Core w polskiej wersji językowej lub produkt równoważny:**

**2 licencje** oprogramowania (typu 16-core licenses) dla instytucji samorządowych, na nośniku CD/DVD lub udostępnienie oprogramowania drogą elektroniczną poprzez dostęp do strony internetowej zawierającej dane oprogramowanie. Licencja – bez ograniczeń czasowych.

Warunki licencjonowania muszą zezwalać na:

* korzystanie oprogramowania na trzech fizycznych serwerach posiadając dwa procesory po 6 rdzeni,
* zmianę wersji systemu operacyjnego na niższą (tzw. downgrade) w celu wykorzystania posiadanych licencji dostępowych Windows Server CAL dla wersji systemu serwerowego Microsoft Windows Server 2012 z zachowaniem wsparcia technicznego,
* przeniesienie licencji systemu operacyjnego na inny fizyczny serwer.

| **Lp.** | **Warunek równoważności** |
| --- | --- |
|  | Współpraca z procesorami o architekturze x86-64. |
|  | Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym. |
|  | Obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych). |
|  | Pojemność obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego - co najmniej 4TB. |
|  | Zawarta możliwość uruchamiania nieograniczonej wirtualnych instancji systemu operacyjnego. |
|  | Obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu. |
|  | Praca w roli klienta domeny Microsoft Active Directory. |
|  | Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2012. |
|  | Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP). |
|  | Zawarta możliwość uruchomienia roli serwera DNS. |
|  | Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP). |
|  | Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. |
|  | Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. |
|  | Zawarta możliwość uruchomienia roli serwera stron WWW. |
|  | W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera. |
|  | W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych. |
|  | W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego. |
|  | Wszystkie wymienione w tabeli parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów). |

## **11. Licencja dostępowa Microsoft Standard 2016 typu CAL User lub produkt równoważny:**

**Licencja** w celu usług dostępowych typu na użytkownika do oprogramowania Microsoft Windows Server 2019 z dożywotnią licencją użytkowania.

|  |  |
| --- | --- |
| **Lp.** | **Warunek równoważności** |
|  | Licencja równoważna musi zezwalać na pracę w systemie Microsoft Active Directory. |