**ZAŁĄCZNIK NR 7 DO SIWZ**

DLA PRZETARGU NIEOGRANICZONEGO

NR 34/DU/Z/13

numery tabel (X.X.X.X) zgodne z numerami stosowanymi w OPZ

*kolumny „Proponowane rozwiązanie” i „Proponowana liczba sztuk” wypełnia Oferent, kolumny „Spełnienie wymagań” - Zamawiający*



#### Wymagania szczegółowe dla stosowanych produktów – routery

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Routery brzegowe | Wymagania dotyczą:  RTR.NET.CG  RTR.NET.CZ | Router musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania w szafie rack, wyposażonym w wymienny zasilacz oraz wentylatory. Router musi być wyposażony w zasilacze dostosowane do napięcia 220-230V, w ilości umożliwiającej poprawną pracę Routera w pełnej konfiguracji przy obsadzeniu wszystkich dostępnych slotów modułami z interfejsami.  Router musi być wyposażony w nadmiarowe zasilacze w celu uzyskania redundancji zasilania 1:1.  Zarządzanie i konfiguracja routera przez administratorów musi być realizowana przez moduł kontrolny. System operacyjny routera musi być instalowany i uruchamiany na module kontrolnym. Moduł kontrolny musi odpowiadać ze sterowanie i monitorowanie pracy komponentów urządzenia. Ruch tranzytowy użytkowników przechodzący przez router nie może być przesyłany przez moduł kontrolny. Moduł kontrolny musi być wyposażony w co najmniej 2 GB pamięci RAM, pamięć Flash, port konsoli oraz interfejs Ethernet służący do zarządzania out-of-band. Moduł kontrolny musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego routera z nośnika danych podłączonego do slotu USB na module kontrolnym.  Router musi być wyposażony w dwa sprzętowe moduły kontrolne w celu zapewnienia redundancji.  System operacyjny routera musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł routingu IP, odpowiedzialny za ustalenie tras routingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. Obsługa ruchu tranzytowego użytkowników musi być realizowana sprzętowo.  Router musi obsługiwać interfejsy 10 Gigabit Ethernet zgodne z IEEE 802.3ae. Router musi być dostarczony z 6 interfejsami 10 Gigabit Ethernet XFP/Xenpack/X2/SFP+. Urządzenie musi umożliwiać rozbudowę do 8 interfejsów 10 Gigabit Ethernet.  Router musi obsługiwać interfejsy 1 Gigabit Ethernet SFP. Router musi być dostarczony z 20 interfejsami Gigabit Ethernet SFP. Urządzenia musi obsługiwać moduły SFP o prędkościach 1 Gb/s i 100 Mb/s. Urządzenie musi umożliwiać rozbudowę do min. 40 interfejsów Gigabit Ethernet.  Router mieć przepustowość nie mniejszą niż 80 Gbps full duplex dla długich pakietów oraz nie mniej niż 55 milionów pakietów na sekundę.  Router musi obsługiwać ramki Jumbo o wielkości 9 KB.  Porty GbE i 10 GbE urządzenia muszą obsługiwać mechanizm Digital Optical Monitoring (DOM).  Urządzenie musi obsługiwać w sprzęcie routing IPv4, IPv6 oraz MPLS.  Urządzenie musi obsługiwać routing statyczny IPv4 oraz routing dynamiczny IPv4 – co najmniej dla protokołów routingu OSPF, IS-IS i BGP.  Urządzenie musi obsługiwać routing statyczny IPv6 oraz routing dynamiczny IPv6 – co najmniej dla protokołów routingu OSPF, IS-IS i BGP.  Router jednocześnie musi obsługiwać nie mniej niż 900 tysięcy wpisów w tablicy routingu IPv4, 900 tysięcy wpisów w tablicy VPN IPv4, 700 tysięcy wpisów w tablicy routingu IPv6 oraz 128 tysięcy adresów MAC.  Router jednocześnie musi obsługiwać nie mniej niż 900 tysięcy wpisów w tablicy routingu IPv4, 512 tysięcy wpisów w tablicy routingu IPv6 oraz 128 tysięcy adresów MAC.  Router musi mieć możliwość rozbudowy (sprzętowej lub licencyjnie) do obsługi mechanizmu tworzenia wirtualnych routerów (kontekstów, routerów logicznych) umożliwiający routing pakietów w oparciu o niezależne tablice routingu – musi m.in. umożliwiać uruchomienie nie mniej niż 5 instancji routingu BGP dla różnych numerów systemów autonomicznych. Router musi obsługiwać sprzętowo 3 pełne tablice BGP dla IPv4 dla 3 różnych numerów systemów autonomicznych (przy założeniu, że w pełnej tablicy BGP znajduje się 300 tysięcy prefiksów). Router musi obsługiwać nie mniej niż 500 sesji BGP.  Router musi obsługiwać protokół redundancji VRRP.  Mechanizm BFD musi być obsługiwany dla IPv4, IPv6 oraz MPLS LSP.  Urządzenie musi posiadać funkcję filtrowania ruchu wchodzącego i wychodzącego z wszystkich interfejsów. Filtrowanie ruchu musi odbywać się co najmniej na podstawie adresów MAC, IPv4 i IPv6. Router musi obsługiwać nie mniej niż 10 000 reguł filtrowania ruchu. Włączenie filtrowania nie może powodować degradacji wydajności urządzenia, tzn. musi być realizowane sprzętowo z prędkością łącza.  Router musi obsługiwać protokół SNMP w wersjach 1, 2 i 3. Router musi udostępniać za pomocą protokołu SNMP co najmniej 64 bitowe liczniki ramek i bajtów wysłanych i odebranych na poszczególnych interfejsach tranzytowych. Router musi udostępniać za pomocą protokołu SNMP liczniki odebranych ramek zawierających błędy na poszczególnych interfejsach tranzytowych. Router musi udostępniać za pomocą CLI liczniki ramek wysłanych, odebranych oraz zawierających błędy na poszczególnych interfejsach tranzytowych. Ponadto po SNMP muszą być dostępne liczniki pakietów i bajtów przechwyconych przez poszczególne filtry ruchu (ACL).  Router musi posiadać mechanizmy pozwalające na ograniczanie pasma dla ruchu wyjściowego i wejściowego na wszystkich interfejsach tranzytowych (z uwzględnieniem filtrów ruchu – ACL) oraz dla poszczególnych sieci VLAN.  Router musi posiadać mechanizmy klasyfikowania ruchu, jego filtrowanie oraz znakowanie w oparciu co najmniej 802.1p, DSCP, ToS, MPLS EXP na wszystkich portach tranzytowych oraz dla poszczególnych sieci VLAN. Dodatkowo klasyfikacja pakietów musi się również odbywać o dane z protokołu BGP – nie mniej niż Community i AS Path. Znakowanie pakietów musi być wykonywane również przez tri-colored policer.  Urządzenie musi wykonywać shaping lub policing ruchu per port.  Router musi obsługiwać co najmniej 8 kolejek wyjściowych dla każdego portu tranzytowego. Urządzenie musi posiadać możliwość buforowania do 100 ms na wszystkich portach tranzytowych. Router musi obsługiwać mechanizm WRED.  Router musi mieć zaimplementowane tunelowanie GRE oraz IP-IP bezpośrednio na karcie liniowej o wydajności przynajmniej 1Gbps.  Router musi obsługiwać ruch IP multicast – w zakresie co najmniej protokołów IGMP (wersje 1, 2, 3) oraz PIM-SM.  Na wszystkich interfejsach przeznaczonych do obsługi ruchu tranzytowego urządzenia musi obsługiwać usługi MPLS – nie mniej niż L2 VPN, VPLS (oparte o LDP i BGP) oraz BGP/MPLS VPN (L3 VPN).  Router musi obsługiwać nie mniej niż 2000 sieci VPLS.  Dla L2 VPN oraz VPLS musi być obsługiwany multihoming.  Router musi obsługiwać protokół sygnalizacji RSVP-TE z mechanizmem Fast Reroute (node protection oraz link protection).  Router musi posiadać możliwość uruchomienia mechanizmu DiffServ Traffic Engineering w celu przekierowania ruchu należącego do różnych klas obsługi ruchu na różne ścieżki MPLS.  W ramach IPVPN ruch multicast musi być obsługiwany wykorzystując sygnalizację BGP oraz w zakresie transportu MPLS point-to-multipoint według draft-ietf-l3vpn-2547bis-mcast-bgp-03.txt, draft draft-ietf-l3vpn-2547bis-mcast-02.txt, Requirements for Multicast in Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs) RFC4834 oraz draft-ietf-l3vpn-mvpn-considerations-01  Urządzenie musi obsługiwać sieci VLAN zgodnie z IEEE 802.1q. Urządzenie musi pozwalać na skonfigurowanie i uruchomienie nie mniej niż 4094 sieci VLAN jednocześnie.  Urządzenie musi obsługiwać mechanizm Q-in-Q włącznie z funkcją terminowania wewnętrznych sieci VLAN na interfejsach warstwy trzeciej.  Router musi wspierać 802.1ah (Provider Backbone Bridge).  Urządzenie musi obsługiwać protokoły Spanning Tree – zgodnie z co najmniej IEEE 802.1d, 802.1w i 802.1s.  Ramki BPDU pomiędzy sieciami VLAN muszą być przenoszone przez urządzenie również w trybie MPLS/VPLS.  Urządzenie musi obsługiwać pracę w architekturze pierścienia z możliwością przerwania pierścienia w różnych miejscach dla różnych sieci wirtualnych (np. z wykorzystaniem Per VLAN Spanning Tree Protocol). Urządzenie musi umożliwiać szybkie przywrócenie (nie dłużej niż 1 sekunda) komunikacji w pierścieniu składającym się z co najmniej 100 urządzeń.  Router musi być zarządzany poprzez tekstowy interfejs linii komend (CLI) dostępny po porcie konsoli, oraz protokół Telnet i SSH dostępny przez interfejs do zarządzania out-of-band oraz dowolny interfejs tranzytowy. Router musi posiadać funkcję współpracy z zewnętrznymi serwerami AAA RADIUS (RFC 2138, RFC 2139) oraz TACACS+ (RFC 1492).  Router musi posiadać funkcję limitowania pasma dla usług, których działania jest niezbędne do prawidłowego działania urządzenia, a które mogą stać się celem ataku Denial of Service.  Urządzenia musi mieć domyślnie zaimplementowane zabezpieczenia przed atakami na poziomie protokołu ARP – minimalny wymagany poziom zabezpieczeń to limitowanie ruchu ARP. |  |  |  |  |

*Tabela 1 Routery brzegowe*



#### Wymagania szczegółowe dla stosowanych produktów – firewalle zewnętrzne

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Firewalle zewnętrzne | Wymagania dotyczą:  FWZ.NET.CG oraz FWZ.NET.CZ | 1. Zewnętrzne zapory sieciowe, system ochrony przed intruzami, system filtrowania treści i ochrony ruchu HTTP(S) muszą tworzyć system zabezpieczeń dostarczony jako klaster HA złożony z dwóch dedykowanych urządzeń zabezpieczeń sieciowych (appliance).. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta. 2. System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej. 3. Urządzenie zabezpieczeń musi posiadać przepływność nie mniej niż 25 Gb/s dla kontroli firewall, nie mniej niż 12 Gb/s dla kontroli IPS i obsługiwać nie mniej niż 2 000 000 jednoczesnych połączeń. 4. Urządzenie zabezpieczeń musi być wyposażone w co najmniej 10 portów Ethernet 10/100/1000. Musi być możliwość zamontowania w urządzeniu minimum 12 interfejsów optycznych gigabit (SFP) oraz minimum 6 interfejsów optycznych 10 gigabit (SFP+). 5. Razem z każdym urządzeniem zabezpieczeń dostarczone muszą być cztery wkładki SFP+ SR i dwie SFP+ LR 6. System zabezpieczeń musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI). 7. Polityka bezpieczeństwa Firewall w zakresie kontroli ruchu sieciowego uwzględnia kierunek przepływu pakietów, protokoły, usługi sieciowe, użytkowników i serwery usług, stan połączenia oraz dane aplikacyjne (m.in. obsługuje fragmentację IP, ochronę systemu operacyjnego przed atakami Exploit i DoS). Ponadto polityka kontroli umożliwia definiowanie zasad wykorzystania aplikacji przez użytkowników niezależnie od stosowanych przez aplikacje numerów portów i protokołów komunikacyjnych. Baza wzorców unikalnych aplikacji zawiera ponad 4500 pozycji, a baza Widget’ów Web 2.0 ponad 200000 pozycji. 8. Firewall bez dodatkowych aplikacji umożliwia szczegółową kontrolę aplikacji sieciowych (m.in. kontroluje schematy i adresację URL, blokuje niedozwolone załączniki w stronach HTML jak ActiveX i Java, blokuje niedozwolone pliki kopiowane poprzez HTTP, blokuje URL zawierające niedozwolone słowa, kontroluje rozmiar przesyłek pocztowych, blokuje Mail Relaying, blokuje niedozwolone pliki przesyłane jako załączniki do poczty). 9. Elementy węzła realizujące funkcjonalność firewall muszą być zbudowane w oparciu o klaster dwu urządzeń mogących pracować w trybie active / passive i active / active 10. Funkcjonalność klastra dwu urządzeń pracujących w trybie active/active musi być realizowana w oparciu o mechanizmy wbudowane w klaster (bez udziału zewnętrznych urządzeń typu load balancer, dynamicznego protokołu routingu lub wykorzystania wirtualizacji) 11. Uwierzytelnianie w sieci VPN odbywa się za pomocą certyfikatów cyfrowych wydawanych przez centralny system zarządzania oraz w razie potrzeby przez zewnętrzny urząd certyfikacji. 12. Centralny system zarządzania dla systemu zabezpieczeń posiada wbudowany wewnętrzny urząd certyfikacji (CA) do wydania certyfikatów VPN. Zarządzanie systemu zabezpieczeń oraz CA odbywa się z tej samej konsoli GUI. 13. System zabezpieczeń posiada trójwarstwową architekturę - moduł zabezpieczeń Firewall, moduł zarządzania i interfejs GUI. Komunikacja pomiędzy modułem zabezpieczeń Firewall i modułem zarządzania jest szyfrowana i uwierzytelniona z użyciem certyfikatów cyfrowych 14. Urządzenia firewall wchodzące w skład węzła muszą mieć możliwość obsłużenia minimum 1024 sieci VLAN (min. 256 na pojedynczym interfejsie) 15. Urządzenia firewall wchodzące w skład węzła muszą obsługiwać routing dynamiczny RIP oraz OSPF 16. Urządzenia firewall wchodzące w skład węzła muszą mieć możliwość inspekcji protokołów HTTP oraz FTP na portach innych niż standardowe 17. Urządzenia firewall wchodzące w skład węzła muszą mieć możliwość wdrożenia mechanizmów Quality of Service (QoS) 18. Urządzenia firewall wchodzące w skład węzła muszą mieć współpracować z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołu RADIUS oraz TACACS 19. System zabezpieczeń musi działać zgodnie z zasadą tzw. minimalnego koniecznego dostępu, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki firewall zabezpieczeń są wskazane jako dozwolone. 20. System zabezpieczeń musi identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i techniki obchodzenia systemów kontroli (włącznie z P2P i IM). 21. System musi umożliwiać identyfikowanie niedozwolonych lub podejrzanych działań, prób ataku oraz po ich wykryciu podnosi alarm (m.in. wykrywa skanowanie portów, IP Spoofing, SYN Flood, CodRad, Nimda). 22. Liczba jednocześnie obsługiwanych przez firewall sesji może być ograniczona jedynie wydajnością platformy sprzętowej. 23. System musi umożliwiać dynamiczną i statyczną translację adresów NAT. Reguły NAT muszą być generowane automatycznie lub definiowane ręcznie. 24. System musi umożliwiać uwierzytelnianie administratorów za pomocą haseł statycznych, haseł dynamicznych lub certyfikatów cyfrowych. Wymagana jest możliwość definiowania szczegółowych uprawnień administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkowników). 25. System zabezpieczeń transparentnie ustala tożsamość użytkowników sieci (integracja z kontrolerem domeny AD). Uwierzytelnianie transparentne oznacza, że użytkownik nie musi podawać swojego identyfikatora i hasła w systemie zabezpieczeń. Polityka kontroli dostępu musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i aplikacji (w tym P2P, IM, Facebook), tzn. umożliwiać różnicowanie polityki kontroli dostępu do aplikacji pomiędzy różnymi kategoriami (grupami) użytkowników na podstawie ich przynależności do poszczególnych grup w LDAP/AD, oraz bez konieczności stosowania dodatkowych urządzeń sieciowych lub instalacji jakiegokolwiek oprogramowania agenckiego po stronie komputera użytkownika. 26. System musi posiadać możliwość obsługi zdalnych użytkowników łączących się za pomocą IPSec, SSL VPN oraz L2TP 27. System zabezpieczeń musi identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. 28. System zabezpieczeń musi być dostarczony z modułem wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS) oraz modułem inspekcji antywirusowej, kontrolującym przynajmniej pocztę elektronicznej (SMTP, POP3, IMAP), FTP oraz HTTP i HTTPS bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza AV musi być przechowywania na urządzeniu i regularnie aktualizowana w sposób automatyczny. 29. System zabezpieczeń musi być dostarczony z modułem filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza WF musi być przechowywania na urządzeniu i regularnie aktualizowana w sposób automatyczny .   Wraz z produktem wymagane jest dostarczenie opieki technicznej. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz jego autoryzowanego polskiego przedstawiciela, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, aktualizację bazy ataków IPS, definicji wirusów, definicji aplikacji a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. |  |  |  |  |

Tabela 2 Firewalle zewnętrzne

#### Wymagania szczegółowe dla stosowanych produktów – firewalle wewnętrzne

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Firewalle wewnętrzne | Wymagania dotyczą:  FWW.NET.CG oraz FWW.NET.CZ | 1. Centralna zapora sieciowa musi być dostarczona jako dedykowane urządzenie w obudowie modularnej, przystosowanej do montażu w szafie rack, wyposażone w pasywny midplane, wymienne wentylatory, wewnętrzne zasilacze z zapewnieniem redundancji zasilania. 2. Urządzenie musi posiadać wymienne karty z matrycą przełączającą, karty z interfejsami sieciowymi oraz dedykowane karty usługowe realizujące funkcje bezpieczeństwa. 3. Urządzenie musi posiadać minimum 8 slotów umożliwiających instalację kart liniowych lub kart usługowych. 4. Urządzenie musi być dostarczone z matrycą przełączającą posiadającą wewnętrzne połączenie z wszystkimi kartami z interfejsami sieciowymi oraz wszystkimi kartami usługowymi. Przepustowość matrycy przełączającej nie może być niższa niż 320 Gb/s. 5. Urządzenie musi obsługiwać co najmniej następujące rodzaje kart z interfejsami sieciowymi: nie mniej niż 16-portowe Gigabit Ethernet (miedziane oraz SFP) oraz nie mniej niż 2-portowe 10 Gigabit Ethernet XFP/SFP+/Xenpack. Urządzenie musi umożliwiać zainstalowanie nie mniej niż 6 kart z interfejsami sieciowymi. Karty muszą posiadać przepustowość co najmniej 10 Gb/s full duplex. Mechanizmy QoS (policing, kolejkowanie) muszą być realizowane sprzętowo. Do sprzętowej obsługi tych funkcji dopuszczalne jest zastosowanie dedykowanych oddzielnych kart o przepustowości nie mniejszej niż 10 Gb/s, nie będących kartami interfejsów. Urządzenie musi być dostarczony z 2 interfejsami 10 Gigabit Ethernet LR oraz 12 portami 1Gigabit Ethernet (w tym 4 definiowane przez moduły SFP – należy dostarczyć 2 wkładki 1000Base-LX). Urządzenie musi umożliwiać rozbudowę o kolejne 4 interfejsy 10 Gigabit Ethernet. 6. Realizacja mechanizmów bezpieczeństwa musi się odbywać na wyspecjalizowanych kartach usługowych posiadających własny procesor. Karty usługowe muszą realizować sprzętowo co najmniej takie funkcje jak stateful firewall, IPSec VPN, intrusion prevention (IPS). Zwiększenie wydajności ww. funkcji bezpieczeństwa musi się odbywać przez zwiększanie ilości kart usługowych. Urządzenie musi posiadać minimum 8 uniwersalnych slotów pozwalających na zainstalowanie i uruchomienie minimum 4 karty serwisowe. 7. Urządzenie musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci z wydajnością nie mniejszą niż 10 Gb/s liczoną dla dużych pakietów oraz 5 Gbps dla ruchu IMIX (wydajność w pełni niezależna od funkcjonalności opisanych w pkt 9 i 10). Firewall musi przetworzyć nie mniej niż 1,5 miliony pakietów/sekundę (dla pakietów 64-bajtowych). Firewall musi obsłużyć nie mniej niż 1,5 milionów równoległych sesji oraz zestawić nie mniej niż 80 tysięcy nowych połączeń/sekundę. 8. System operacyjny firewalla musi śledzić stan sesji użytkowników (stateful processing), tworzyć i zarządzać tablicą stanu sesji. 9. Urządzenie musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site z wydajnością minimum 4 Gbps (wydajność w pełni niezależna od funkcjonalności opisanych w pkt 7 i 10). IPSec VPN musi być realizowany sprzętowo przez dedykowane karty usługowe. 10. Urządzenie musi posiadać funkcję wykrywania i blokowania ataków intruzów (IPS, intrusion prevention) realizowaną na modułach usługowych. System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące DDoS oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych ataków (intruzów, robaków) musi odbywać się w regułach polityki bezpieczeństwa. Urządzenie musi realizować zadania IPS z wydajnością nie mniejszą niż 4 Gb/s w trybie inline (wydajność w pełni niezależna od funkcjonalności opisanych w pkt 7 i 9). Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall. Baza sygnatur ataków musi być aktualizowana przez producenta minimum jeden raz w tygodniu. Funkcjonalność IPS musi być realizowana przez dedykowane karty usługowe. 11. Urządzenie musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF oraz BGP. Urządzenie musi obsługiwać nie mniej niż mniej niż 1 000 000 wpisów routingowych Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 250 wirtualnych routerów (również na poziomie funkcji firewalla) oraz 1 000 sieci VLAN z tagowaniem 802.1Q. 12. Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków TCP i UDP. Urządzenie musi posiadać tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach. 13. Urządzenie musi posiadać możliwość pracy w konfiguracji odpornej na awarie np. w klastrze funkcjonującym w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. 14. Zarządzanie urządzeniem musi odbywać się za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH. Urządzenie musi posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta. 15. Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji. 16. Musi zostać zestawiony klaster niezawodnościowy z wykorzystaniem 2 łączy 1000BaseLX – w celu przesyłu sygnalizacji synchronizacyjnej między elementami klastra. Jeżeli w proponowanej technologii zarówno dane jak i synchronizacja odbywa się po łączach 10Gb – należy zastosować w miejsce 2 łączy 1000BaseLX dodatkowe łącza 10Gb (w takim przypadku Urządzenie musi być wyposażony w minimum 2 porty 10Gb LR, interfejsy SFP nie muszą być obsadzone wkładkami 1000BaseLX). |  |  |  |  |

Tabela 3 Firewalle wewnętrzne



#### Wymagania szczegółowe dla stosowanych produktów – przełączniki dla strefy DMZ

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Przełączniki dla strefy DMZ | Wymagania dotyczą:  SWDMZ.NET.CG  SWDMZ.NET.CZ | 1. Przełącznik musi posiadać minimum 48 portów GigabitEthernet 10/100/1000 BaseT oraz minimum 2 porty SFP+ 10Gb. 2. Przełącznik musi być wyposażony w minimum 256MB pamięci DRAM oraz 128 MB pamięci flash. 3. Przełącznik musi posiadać przepustowość min. 88 Gb/s, wydajność przełączania przynajmniej 65 Mpps 4. Przełącznik musi obsługiwać VLAN 802.1q. 5. Przełącznik musi obsługiwać STP (z możliwością uruchomienia instancji per-vlan), RSTP, MSTP. 6. Przełącznik musi obsługiwać agregację portów w grupy zgodnie z LACP (min. 8 portów per grupa). 7. Przełącznik musi zapewniać przełączanie w warstwie trzeciej oraz definiowanie routingu w oparciu o protokoły RIPv1v2, routing statyczny i OSPF. 8. Przełącznik musi umożliwiać rozszerzenie oprogramowania do obsługi protokołu routingu dynamicznego BGP-4 oraz IS-IS. 9. Przełącznik musi zapewniać podstawową obsługę ruchu IP Multicast, w tym funkcjonalność IGMP v1, v2, v3 oraz IGMP Snooping. 10. Przełącznik musi posiadać możliwość obsługi IP Multicast z wykorzystaniem protokołów PIM-SM, PIM-SSM, PIM-DM. 11. Przełącznik musi posiadać możliwość obsługi funkcjonalności PBR (Policy Based Routing) lub równoważnej. 12. Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP: DHCP Server oraz DHCP Relay. 13. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci: 14. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP 15. Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Round Robin lub podobnego dla obsługi tych kolejek 16. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority) 17. Obsługa IP Precedence i DSCP. 18. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci: 19. Wiele poziomów dostępu administracyjnego poprzez konsolę 20. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1x oraz EAP 21. Możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2 22. Możliwość definiowania listy kontroli dostępu (ACL) na poziomie portów (PACL), VLAN-ów (VACL), interfejsów routera (RACL) 23. Obsługa DHCP snooping 24. Obsługa dynamicznej inspekcji ARP. 25. Przełącznik musi mieć możliwość synchronizacji zegara czasu za pomocą protokołu NTP. 26. Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) powinien być możliwy do edycji w trybie off-lin. tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania 50 plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne bez częściowych restartów urządzenia po dokonaniu zmian. 27. Przełącznik musi posiadać możliwość tworzenia stosu o przepustowości pomiędzy elementami stosu (backplane) co najmniej 64 Gbps. Urządzenia w stosie muszą współdzielić wspólną tablice MAC oraz routingu, musi istnieć zestawienie połączeń typu channel do różnych przełączników w obrębie stosu. Stos musi być widoczny z punktu widzenia zarządzania jako jedno urządzenie. 28. Przełącznik musi posiadać możliwość tworzenia stosu łączącego co najmniej 9 urządzeń. 29. Przełącznik musi posiadać możliwość tworzenia stosu z przełącznikami dostępowymi 30. Przełącznik musi umożliwiać kopiowanie ruchu (z portu, VLANu) na określony port (mirror). 31. Przełącznik musi być wyposażony w redundantny wewnętrzny zasilacz. 32. Tablica CAM musi obsłużyć min. 6 000 adresów MAC. 33. Przełącznik musi obsługiwać min. 1024 VLANy. 34. Tablica routingu musi obsłużyć min. 8 000 wpisów (dla adresów unicast IPv4). 35. Przełącznik musi mieć możliwość rozbudowy o sprzętową obsługę IPv6. Po rozbudowie musi istnieć możliwość obsługi min. RIPng, OSPFv3, PIM, MLD, MLDv2. 36. Przełącznik musi obsługiwać mechanizm VRF lub VRF lite. 37. Przełącznik musi mieć możliwość pracy jako samodzielne urządzenie. |  |  |  |  |

Tabela 4 Przełączniki dla strefy DMZ



#### Wymagania szczegółowe dla stosowanych produktów – Zewnętrzny system terminowania połączeń SSLVPN

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Zewnętrzny system do terminowania połączeń SSL VPN | Wymagania dotyczą:  SSL.NET.CG SSL.NET.CZ | 1. Bramka SSL VPN musi posiadać co najmniej 2 porty 1 GbE Copper 2. Bramka SSL VPN musi posiadać redundantne zasialnie. 3. Bramka SSL vPN musi być nie większa niż 1U. 4. Bramka SSL VPN musi być przystosowana do montażu w szafie rack. 5. Bramka SSL VPN musi umożliwić terminację VPN typu remote access w oparciu o certyfikaty i architekturę PKI 6. Bramka SSL VPN musi zapewnić sterowanie uprawnieniami do zasobów sieciowych w oparciu o grupy 7. Bramka SSL VPN musi być dedykowanym urządeniem sieciowym 8. Bramka SSL VPN musi potrafić pracować w trybie active/active lub active/passive 9. Bramka SSL VPN musi obsłużyc minimalnie 25 użytkowników jednocześnie. |  |  |  |  |

Tabela 5 Zewnętrzny system terminowania połączeń SSLVPN



#### Wymagania szczegółowe dla stosowanych produktów – system zarządzania dostępem do sieci (Network Admission Control)

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| System zarządzania dostępem do sieci  (Network Admission Control) | Wymagania dotyczą:  NAC.NET.CG NAC.NET.CZ | 1. W system musi być wbudowany serwer RADIUS    1. Musi istnieć możliwość zarządzania atrybutami zwracanymi przez serwer RADIUS    2. Musi być możliwość autoryzacji z użyciem MAC RADIUS 2. System musi umożliwiać bezpośrednią integrację z LDAP oraz Active Directory 3. System musi umożliwiać automatyczną autoryzację urządzeń i użytkowników domenowych 4. System musi umożliwiać zwracanie zadeklarowanych atrybutów RADIUS w zależności od tego czy użytkownik wykorzystuje komputer domenowy 5. System musi umożliwiać zwracanie zadeklarowanych atrybutów RADIUS w zależności od tego czy użytkownik wykorzystuje urządzenia spoza domeny Active Directory 6. Możliwość tworzenia polityk dostępowych przez przypisanie VLANu lub zwrócenie dowolnego zestawu atrybutów RADIUS, na podstawie wyniku uwierzytelnienia 7. System musi obsługiwać nie mniej niż 5000 jednoczesnych sesji RADIUS 8. System zarządzania dostępem do sieci (Network Admission Control) musi być w pełni kompatybilny z Przełącznikami centralnymi, przełącznikami z Punktów dystrybucyjnych oraz siecią bezprzewodową |  |  |  |  |

Tabela 6 System zarządzania dostępem do sieci (Network Admission Control)

#### Wymagania szczegółowe dla stosowanych produktów – przełączniki centralne

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Przełączniki centralne | Wymagania dotyczą:  SWR.NET.CG SWR.NET.CZ | 1. Ilość interfejsów – minimum 40 interfejsów 10Gb definiowanych przez wkładki 10GBaseX SFP+ lub Xenpack lub X2, w tym 2 interfejsy z dostarczonymi wkładkami 10Gb-LR. 2. Przełącznik musi mieć możliwość instalacji zarówno portów 1Gb jak i 10Gb. 3. Przełącznik może być urządzeniem typu standalone lub przełącznikiem modularnym. W przypadku zastosowania przełącznika modularnego wymagane jest aby każda karta liniowa posiadała możliwość przełączania lokalnego dla ruchu L2 i L3 bez konieczności przesyłania ruchu lokalnego przez moduł zarządzający lub matrycę przełączającą zainstalowaną poza kartą liniową. W przypadku zastosowania przełącznika modularnego wymagane jest aby każda karta liniowa pracowała bez nadsubskrypcji. 4. Przepustowość – minimum 720 Gbps w trybie fullduplex. 5. Wydajność – minimum 450 Mpps dla IPv4 Routing oraz Layer 2 Bridging. 6. Musi być wyposażony w minimum 1GB pamięci DRAM oraz 1GB pamięci flash. 7. Musi być wyposażony w minimum 2 redundantne zasilacze. 8. Musi obsługiwać minimum 8 kolejek QoS na 1 port. 9. Musi obsługiwać minimum 24 000 adresów MAC. 10. Musi obsługiwać Jumbo Frames 9216 Bytes. 11. Musi obsługiwać co najmniej 4096 VLANów. 12. Musi zapewniać przełączanie w warstwie trzeciej oraz definiowanie routingu w oparciu o protokoły RIPv1v2, routing statyczny i OSPF. 13. Musi umożliwiać rozszerzenie oprogramowania do obsługi protokołu routingu dynamicznego BGP-4 oraz IS-IS. 14. Musi zapewniać podstawową obsługę ruchu IP Multicast, w tym funkcjonalność IGMP oraz IGMP Snooping. 15. Musi posiadać możliwość obsługi IP Multicast z wykorzystaniem protokołu PIM w trybach SM oraz SSM. 16. Tablica routingu musi obsłużyć min. 8 000 wpisów (dla adresów unicast IPv4). 17. Musi wspierać skonfigurowanie 2 przełączników w jeden przełącznik wirtualny: 18. Obydwa przełączniki wchodzące w skład przełącznika wirtualnego muszą współdzielić tablicę CAM 19. Obydwa przełączniki wchodzące w skład przełącznika wirtualnego muszą współdzielić tablicę routingu 20. Musi istnieć możliwość zestawiania połączenia typu Ethernet channel do przełącznika wirtualnego w skład którego wchodzą połączenia do różnych przełączników w ramach przełącznika wirtualnego. 21. Przełącznik musi obsługiwać mechanizm VRF lub VRF lite. 22. Przełącznik musi mieć możliwość pracy jako samodzielne urządzenie. 23. Przełącznik musi obsługiwać mechanizm Bidirectional Forwarding Detection (BFD). |  |  |  |  |

Tabela 7 Przełączniki centralne

#### 9.1.7.6 Wymagania szczegółowe dla stosowanych produktów – punkty dystrybucyjne

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Punkty dystrybucyjne | Wymagania dotyczą:  Wszystkie przełączniki w Punktach dystrybucyjnych | 1. Przełączniki muszą pochodzić od jednego producenta oraz z jednej linii produktowej 2. Możliwość łączenia minimum 9 urządzeń w jednym stosie. Stos może być zbudowany z dowolnych przełączników opisanych w niniejszym punkcie |  |  |  |  |

Tabela 8 Punkty dystrybucyjne. Część 1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| Punkty dystrybucyjne | Wymagania dotyczą:  SWD1.NET.B-CG  SWD2.NET.B-CG  SWD1.NET.B-CZ  SWD2.NET.B-CZ  SWD1.NET.B-W1  SWD1.NET.B-W2  SWD1.NET.B-P  SWD1.NET.B-K  SWD1.NET.B-E  SWD1.NET.B-Gn | 1. Przełącznik musi posiadać minimum 24 portów GigabitEthernet 10/100/1000 BaseT, w tym minimum 8 musi posiadać obsługę Power over Ethernet (PoE) zgodnych z 802.3af, dających moc 15.4 W na każdym porcie. 2. Przełącznik musi umożliwiać instalację 2 portów lub modułu 2 portowego 10Gigabit Ethernet (dopuszcza się rozwiązania umożliwiające zamienne wykorzystanie interfejsów GE i 10 GE (np. działające 4 interfejsy GE albo 2 10GE). 3. Przełącznik musi umożliwiać instalację 4 portów lub modułu 4 portowego GigabitEthernet z możliwością definicji styku za pomocą modułów GBIC, SFP lub równoważnych (dopuszcza się rozwiązania umożliwiające zamienne wykorzystanie interfejsów GE i 10 GE (np. działające 4 interfejsy GE albo 2 10GE). 4. Nie dopuszcza się, aby uruchomienie któregokolwiek z portów opisanych w pkt. 2 i 3 powodowało zablokowanie dowolnego z 24 podstawowych portów 10/100/1000 BaseT. 5. Przełącznik musi być wyposażony w minimum 256MB pamięci DRAM oraz 128 MB pamięci flash. 6. Przełącznik musi posiadać przepustowość min. 88 Gb/s, wydajność przełączania przynajmniej 65 Mpps. 7. Przełącznik musi obsługiwać VLAN 802.1q. 8. Przełącznik musi obsługiwać STP (z możliwością uruchomienia instancji per-vlan), RSTP, MSTP). 9. Przełącznik musi obsługiwać agregację portów w grupy zgodnie z LACP (min. 8 portów per grupa). 10. Przełącznik musi zapewniać przełączanie w warstwie trzeciej oraz definiowanie routingu w oparciu o protokoły RIPv1v2, routing statyczny i OSPF. 11. Przełącznik musi umożliwiać rozszerzenie oprogramowania do obsługi protokołu routingu dynamicznego BGP-4 oraz IS-IS. 12. Przełącznik musi zapewniać podstawową obsługę ruchu IP Multicast, w tym funkcjonalność IGMP v1, v2, v3 oraz IGMP Snooping. 13. Przełącznik musi posiadać możliwość obsługi IP Multicast z wykorzystaniem protokołów PIM-SM, PIM-SSM, PIM-DM. 14. Przełącznik musi posiadać możliwość obsługi funkcjonalności PBR (Policy Based Routing) lub równoważnej. 15. Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP: DHCP Server oraz DHCP Relay. 16. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci: 17. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP 18. Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Round Robin lub podobnego dla obsługi tych kolejek 19. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority) 20. Obsługa IP Precedence i DSCP. 21. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci: 22. Wiele poziomów dostępu administracyjnego poprzez konsolę 23. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1x oraz EAP 24. Możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2 25. Możliwość definiowania listy kontroli dostępu (ACL) na poziomie portów (PACL), VLAN-ów (VACL), interfejsów routera (RACL) 26. Obsługa DHCP snooping 27. Obsługa dynamicznej inspekcji ARP. 28. Przełącznik musi mieć możliwość synchronizacji zegara czasu za pomocą protokołu NTP. 29. Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) powinien być możliwy do edycji w trybie off-line tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania 50 plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne bez częściowych restartów urządzenia po dokonaniu zmian. 30. Przełącznik musi posiadać możliwość tworzenia stosu o przepustowości pomiędzy elementami stosu (backplane) co najmniej 64 Gbps. Urządzenia w stosie muszą współdzielić wspólną tablice MAC oraz routingu, musi istnieć zestawienie połączeń typu channel do różnych przełączników w obrębie stosu. Stos musi być widoczny z punktu widzenia zarządzania jako jedno urządzenie. 31. Przełącznik musi posiadać możliwość tworzenia stosu łączącego co najmniej 9 urządzeń. 32. Przełącznik musi posiadać możliwość tworzenia stosu z przełącznikami dostępowymi opisanymi w Tabela 10 Punkty dystrybucyjne. Część 3 33. Przełącznik musi umożliwiać kopiowanie ruchu (z portu, VLANu) na określony port (mirror). 34. Przełącznik musi być wyposażony w redundantny wewnętrzny zasilacz. 35. Tablica CAM musi obsłużyć min. 6 000 adresów MAC. 36. Przełącznik musi obsługiwać min. 1024 VLANy. 37. Tablica routingu musi obsłużyć min. 8 000 wpisów (dla adresów unicast IPv4). 38. Przełącznik musi mieć możliwość rozbudowy o sprzętową obsługę IPv6. Po rozbudowie musi istnieć możliwość obsługi min. RIPng, OSPFv3, PIM, MLD, MLDv2. 39. Przełącznik musi obsługiwać mechanizm VRF lub VRF lite. 40. Przełącznik musi mieć możliwość pracy jako samodzielne urządzenie. |  |  |  |  |

Tabela 9 Punkty dystrybucyjne. Część 2

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Punkty dystrybucyjne | Wymagania dotyczą:  SWD1.NET.B-B,  SWD2.NET.B-B,  SWD1.NET.B-H,  SWD1.NET.B-T3,  SWD1.NET.B-D2,  SWD1.NET.B-T,  SWD1.NET.B-Ls  SWD2.NET.B-Ls  SWD1.NET.B-A,  SWD3.NET.B-B,  SWD1.NET.B-R,  SWD1.NET.B-S8,  SWD1.NET.B-N,  SWD1.NET.B-H2a,  SWD1.NET.B-H3  SWD4.NET.B-B  SWD5.NET.B-B  SWD6.NET.B-B  SWD5.NET.B-CG, SWD6.NET.B-CG  SWD5.NET.B-CZ, SWD6.NET.B-CZ  SWD3.NET.B-CG,  SWD4.NET.B-CG,  SWD3.NET.B-CZ,  SWD3.NET.B-CZ,  SWD2.NET.B-H,  SWD2.NET.B-T3,  SWD2.NET.B-D2,  SWD2.NET.B-T | 1. Przełącznik musi posiadać minimum 48 portów GigabitEthernet 10/100/1000 BaseT, w tym minimum 8 musi posiadać obsługę Power over Ethernet (PoE) zgodnych z 802.3af, dających moc 15.4 W na każdym porcie. 2. Przełącznik musi umożliwiać instalację 2 portów lub modułu 2 portowego 10Gigabit Ethernet (dopuszcza się rozwiązania umożliwiające zamienne wykorzystanie interfejsów GE i 10 GE (np. działające 4 interfejsy GE albo 2 10GE). 3. Przełącznik musi umożliwiać instalację 4 portów lub modułu 4 portowego GigabitEthernet z możliwością definicji styku za pomocą modułów GBIC, SFP lub równoważnych (dopuszcza się rozwiązania umożliwiające zamienne wykorzystanie interfejsów GE i 10 GE (np. działające 4 interfejsy GE albo 2 10GE). 4. Nie dopuszcza się, aby uruchomienie któregokolwiek z portów opisanych w pkt. 2 i 3 powodowało zablokowanie dowolnego z 24 podstawowych portów 10/100/1000 BaseT. 5. Przełącznik musi być wyposażony w minimum 256MB pamięci DRAM oraz 128 MB pamięci flash. 6. Przełącznik musi posiadać przepustowość min. 88 Gb/s, wydajność przełączania przynajmniej 65 Mpps. 7. Przełącznik musi obsługiwać VLAN 802.1q. 8. Przełącznik musi obsługiwać STP (z możliwością uruchomienia instancji per-vlan), RSTP, MSTP). 9. Przełącznik musi obsługiwać agregację portów w grupy zgodnie z LACP (min. 8 portów per grupa). 10. Przełącznik musi zapewniać przełączanie w warstwie trzeciej oraz definiowanie routingu w oparciu o protokoły RIPv1v2, routing statyczny i OSPF. 11. Przełącznik musi umożliwiać rozszerzenie oprogramowania do obsługi protokołu routingu dynamicznego BGP-4 oraz IS-IS. 12. Przełącznik musi zapewniać podstawową obsługę ruchu IP Multicast, w tym funkcjonalność IGMP v1, v2, v3 oraz IGMP Snooping. 13. Przełącznik musi posiadać możliwość obsługi IP Multicast z wykorzystaniem protokołów PIM-SM, PIM-SSM, PIM-DM. 14. Przełącznik musi posiadać możliwość obsługi funkcjonalności PBR (Policy Based Routing) lub równoważnej. 15. Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP: DHCP Server oraz DHCP Relay. 16. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci: 17. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP 18. Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Round Robin lub podobnego dla obsługi tych kolejek 19. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority) 20. Obsługa IP Precedence i DSCP. 21. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci: 22. Wiele poziomów dostępu administracyjnego poprzez konsolę 23. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1x oraz EAP 24. Możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2 25. Możliwość definiowania listy kontroli dostępu (ACL) na poziomie portów (PACL), VLAN-ów (VACL), interfejsów routera (RACL) 26. Obsługa DHCP snooping 27. Obsługa dynamicznej inspekcji ARP. 28. Przełącznik musi mieć możliwość synchronizacji zegara czasu za pomocą protokołu NTP. 29. Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) powinien być możliwy do edycji w trybie off-line tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania 50 plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne bez częściowych restartów urządzenia po dokonaniu zmian. 30. Przełącznik musi posiadać możliwość tworzenia stosu o przepustowości pomiędzy elementami stosu (backplane) co najmniej 64 Gbps. Urządzenia w stosie muszą współdzielić wspólną tablice MAC oraz routingu, musi istnieć zestawienie połączeń typu channel do różnych przełączników w obrębie stosu. Stos musi być widoczny z punktu widzenia zarządzania jako jedno urządzenie. 31. Przełącznik musi posiadać możliwość tworzenia stosu łączącego co najmniej 9 urządzeń. 32. Przełącznik musi posiadać możliwość tworzenia stosu z przełącznikami dostępowymi opisanymi w Tabela 9 Punkty dystrybucyjne. Część 2 33. Przełącznik musi umożliwiać kopiowanie ruchu (z portu, VLANu) na określony port (mirror). 34. Przełącznik musi być wyposażony w redundantny wewnętrzny zasilacz. 35. Tablica CAM musi obsłużyć min. 6 000 adresów MAC. 36. Przełącznik musi obsługiwać min. 1024 VLANy. 37. Tablica routingu musi obsłużyć min. 8 000 wpisów (dla adresów unicast IPv4). 38. Przełącznik musi mieć możliwość rozbudowy o sprzętową obsługę IPv6. Po rozbudowie musi istnieć możliwość obsługi min. RIPng, OSPFv3, PIM, MLD, MLDv2. 39. Przełącznik musi obsługiwać mechanizm VRF lub VRF lite. 40. Przełącznik musi mieć możliwość pracy jako samodzielne urządzenie. |  |  |  |  |

Tabela 10 Punkty dystrybucyjne. Część 3

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Punkty dystrybucyjne | Wymagania dotyczą:  Elementy dodatkowe | 52 modułów SFP+ 10Gb-LR kompatybilnych z przełącznikami z Punktów dystrybucyjnych  48 modułów SFP+ 10Gb-SR kompatybilnych z przełącznikami z Punktów dystrybucyjnych  10 modułów SFP 1000BaseT kompatybilne z przełącznikami centralnymi |  |  |  |  |

Tabela 11 Punkty dystrybucyjne. Część 4



#### Wymagania szczegółowe dla stosowanych produktów – stacja zarządzająca

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Stacja zarządzająca | Wymagania dotyczą:  MGM.NET.CG  MGM.NET | 1. Zdalne zarządzanie i zdalna konfiguracja Urządzeń - tj przełączników (SWDMZ.NET.CG, SWDMZ.NET.CZ, SWR.NET.CG, SWR.NET.CZ, wszystkie przełączniki dostępowe SWDx.NET.Byyy [1..n]) oraz routerów (RTR.NET.CG, RTR.NET.CZ) 2. Możliwość tworzenia wielu użytkowników o różnym poziomie uprawnień do zarządzania różnymi grupami urządzeń (RBAC: Role Based Access Control). 3. Elastyczne metody uwierzytelnienia użytkowników systemu: lokalnie lub przez usługi AAA: LDAP, RADIUS oraz TACACS+ 4. Zapis wybranych przez użytkowników zdarzeń typu SNMP trap i syslog, 5. Oprogramowanie do zarządzania urządzeniami sieci LAN musi stanowić zintegrowany pakiet aplikacji do konfiguracji, administracji, monitoringu i diagnozowania sieci. 6. Musi umożliwiać zarządzanie dostarczanymi urządzeniami, w tym firewall z IDS/IPS. 7. Wymagany ogólny zakres funkcjonalności:    1. Wykrywanie błędów i problemów w czasie rzeczywistym,    2. Wykrywanie urządzeń końcowych i wolnych portów,    3. Narzędzia do zarządzania listą urządzeń (ang. inventory management), oprogramowaniem urządzeń i ich konfiguracją, w tym umożliwiające tworzenie archiwów konfiguracji dla poszczególnych urządzeń,    4. Diagnozowanie stanu, wydajności i dostępności sieci, raportowanie w czasie rzeczywistym oraz w oparciu o dane historyczne,    5. Generowanie szczegółowego opisu użytkowanych urządzeń i ich konfiguracji. 8. Pakiet oprogramowania zarządzającego musi umożliwiać zarządzanie urządzeniami firewall w zakresie:    1. Zarządzania firewallami działającymi na poziomie L3,    2. Zarządzania funkcjami firewalli aplikacyjnych,    3. Definiowanie reguł polityki bezpieczeństwa    4. Definiowanie reguł translacji NAT    5. Konfiguracji mechanizmów QoS na zarządzanych urządzeniach,    6. Konfiguracji rutingu na zarządzanych urządzeniach,    7. Definiowania i konfiguracji usług sieciowych,    8. Konfiguracji, zarządzania i monitoringu funkcjonalności failover,    9. Tworzenia sieci VPN z wykorzystaniem kreatorów,    10. Monitoringu sieci VPN. 9. Pakiet oprogramowania zarządzającego musi umożliwiać zarządzanie urządzeniami IDS/IPS w zakresie:    1. Zarządzania sygnaturami, w tym ich przeglądania, aktywacji/ dezaktywacji, kopiowania i modyfikacji,    2. Przeglądu i tworzenia polityk IDS/IPS,    3. Tworzenia sygnatur IDS/IPS,    4. Automatycznego uaktualniania oprogramowania sond,    5. Monitoringu stanu pracy urządzeń. 10. Pakiet oprogramowania zarządzającego musi umożliwiać zarządzanie przełącznikami  w zakresie:     1. Zarządzania protokołami rutingu,     2. Zarządzania sieciami wirtualnymi (VLAN),     3. Konfiguracji mechanizmów QoS na zarządzanych urządzeniach,     4. Konfiguracji portów urządzenia z wykorzystaniem predefiniowanych profili,     5. Zarządzania rodziną protokołów STP a także zabezpieczania działania STP z wykorzystaniem mechanizmów Root Guard, BPDU Guard, edge port,     6. Konfiguracja ustawień dotyczących bezpieczeństwa portu ang. port security, co najmniej w zakresie limitowania adresów MAC, ARP inspection, DHCP snooping,     7. Zarządzania listami kontroli dostępu. 11. Pełna obsługa systemów logicznych (np. stacki przełączników, grupowanie przełączników w jeden przełącznik wirtualny 12. Stacja zarządzająca może zostać dostarczona w postaci urządzenia appliance lub oprogramowania instalowanego na serwerze ogólnego przeznaczenia. W przypadku oprogramowania należy dostarczyć system operacyjny oraz serwer zgodny z wymaganiami stawianymi przez producenta oprogramowania zarządzającego 13. System zarządzania musi pochodzić z oferty producenta oferowanych przełączników i routerów. 14. System zarządzania musi posiadać licencje potrzebne do zarządzania wszystkimi Urządzeniami - tj przełącznikami (SWDMZ.NET.CG, SWDMZ.NET.CZ, SWR.NET.CG, SWR.NET.CZ, wszystkie przełączniki dostępowe SWDx.NET.Byyy [1..n]), routerami (RTR.NET.CG, RTR.NET.CZ), bramkami SSLVPN – (SSL.NET.CG, SSL.NET.CZ) oraz Firewallami wewnętrznymi (FWW.NET.CG, FWW.NET.CZ) |  |  |  |  |

Tabela 12 Stacja zarządzająca (przełączniki routery, SSLVPN, firewall wewnętrzny)



#### Wymagania szczegółowe dla stosowanych produktów – system antywirusowy

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| System  antywirusowy |  | System antywirusowy:   1. System musi zapewniać bezpieczeństwo fizycznych (Linux, Windows Server 2003/2008/2012 i wirtualnych serwerów (Hyper-V, VMware) oraz stacji użytkowników końcowych Windows XP/. 2. System musi umożliwiać instalację konsoli zarządzającej na systemach Microsoft Windows 3. System musi pozwalać na wybór ochrony agentowej lub bezagentowej w przypadku serwerów wirtualnych, oraz zwirtualizowanych desktopów. 4. System powinien zawierać zaawansowane funkcje zarządzania, upraszczające zakres zadań ochrony. 5. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa. 6. System musi umożliwiać zdefiniowanie harmonogramu lub częstotliwości pobierania aktualizacji wirusów od producenta systemu. 7. System musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa. 8. System musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, itd. 9. System musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów. 10. System musi posiadać możliwość pracy w trybie multi-tenancy, tj. pozwalać na równoległe współistnienie wielu użytkowników posiadających dostęp do widoku jedynie wydzielonej części infrastruktury i zarządzania jej bezpieczeństwem. Użytkownicy powinni mieć możliwość jednoczesnej, bezkonfliktowej w stosunku do siebie pracy z systemem 11. System musi pozwalać na zarządzanie zdarzeniami i natychmiastowe alarmowanie i raportowanie o aktywności wirusów w chronionej infrastrukturze na kilka sposobów 12. Zarządzanie systemem musi odbywać się poprzez standardową przeglądarkę WWW i połączenie https, która nie wymaga instalacji żadnych dodatkowych komponentów. 13. System musi posiadać możliwość powiadamiania o wszystkich zdarzeniach za pomocą poczty elektronicznej, wiadomości SNMP. 14. System musi umożliwiać tworzenie administratorów o różnych stopniach uprawnień w stosunku do różnych modułów i funkcjonalności systemu, a także w stosunku do różnych chronionych obiektów lub grup obiektów. 15. Zarządzanie rolami w systemie musi pozwalać zdefiniowanie uprawnień dających możliwość administrowania wyłącznie jednym chronionym obiektem oraz pojedynczymi funkcjonalnościami systemu 16. System musi pozwalać na tworzenie struktur zarządzanych komputerów również poprzez adresacje IP komputera który podlega zarządzaniu. 17. System musi być przygotowany do pracy w strefie DMZ tak aby było możliwe zarządzanie komputerami znajdującymi się poza siecią korporacyjną. 18. System musi prezentować dane w formie graficznej w panelu głównym 19. System musi umożliwiać na jednoczesny dostęp do konsoli zarządzającej niezależnie przez kilku administratorów. 20. System musi posiadać możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta. 21. System nie może wymagać restartu chronionych komputerów i serwerów po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów. 22. System musi pozwalać na wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”. 23. System musi pozwalać na automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa. 24. System musi zapewniać w procesie skanowania ręcznego i automatycznego przeskanowania dowolnego celu pod względem złośliwego oprogramowania 25. System musi posiadać moduł (aktywowany dedykowaną licencją) pozwalający na wykrywanie ataków typu SQL injection oraz cross-site-scripting. 26. System musi posiadać możliwość przełączania pomiędzy trybem blokowania ruchu i trybem detekcji zdarzeń 27. System musi pełnostanowy firewall (stateful firewall) (aktywowany dedykowaną licencją) pozwalający na łatwą izolacje interfejsów i nie wymagający restartów systemu. 28. System musi umożliwiać kontrolę połączeń wychodzących i przychodzących w komunikacji sieciowej z możliwością kontroli niestandardowych portów TCP.. 29. System musi posiadać możliwość przełączenia trybu działania reguł firewalla z trybu blokowania ruchu w tryb detekcji zdarzeń 30. System musi posiadać predefiniowane reguły chroniące krytyczne elementy chronionych systemów informatycznych. 31. Wszystkie funkcjonalności systemu muszą być zarządzane z jednej, centralnej konsoli. 32. W przypadku ochrony w trybie agentowym wszystkie funkcjonalności systemu muszą być dostępne w ramach pojedynczego agenta instalowanego na chronionych obiektach 33. System musi umożliwiać nanoszenie zmian w profilach bezpieczeństwa w czasie rzeczywistym bez potrzeby restartu systemu i chronionych obiektów. 34. System musi umożliwiać tworzenie dowolnej ilości profilów bezpieczeństwa zawierających predefiniowane reguły ochronne. 35. System musi umożliwiać generowanie na żądanie oraz wg harmonogramu raportów w formatach minimalnie PDF. 36. System musi współpracować z bazami danych Microsoft SQL 37. System musi pozwalać na bezagentową ochronę środowisk wirtualnych opartych o platformę VMware vSphere w wersjach 4.x oraz 5.x |  |  |  |  |

Tabela 13 System antywirusowy



#### Wymagania szczegółowe dla stosowanych produktów – silne uwierzytelnianie oraz SSO

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Silne uwierzytelnianie oraz SSO | SSO.VRT.SCO | 1. Rozwiązanie musi zawierać oprogramowanie systemowe i narzędziowe niezbędne do budowy CA zintegrowanego z domeną Active Directory. 2. Rozwiązanie musi uwzględniać dostawę 500 kart/tokenów USB, które zostaną wykorzystane jako urządzenia uwierzytelniające. 3. Należy dostarczyć serwer, który musi spełniać następujące minimalne wymagania:   - 4xCPU (16 rdzeni)  - 16GB RAM  - 1TB przestrzeni dyskowej dysku  - komplet oprogramowania narzędziowego i systemowego niezbędny do uruchomienia oprogramowania. W przypadku konieczności dostarczenia oprogramowania bazodanowego nie jest dopuszczalne dostarczenie darmowych, ograniczonych wersji np. SQL Server Express czy Oracle Express.   1. Rozwiązanie musi zapewniać integrację z różnymi usługami katalogowymi m.in.:    1. Microsoft Active Directory    2. Microsoft Active Directory Application Mode (ADAM)    3. Microsoft Active Directory Lightweight Directory Services (AD LDS) 2. System musi zapewniać wsparcie dla przeglądarek internetowej:    1. Microsoft Internet Explorer    2. Mozilla Firefox 3. System musi posiadać możliwość zapamiętania danych logowania do:    1. aplikacji Windows,    2. portali webowych – Internet oraz intranet,    3. Microsoft Terminal Server,    4. wsparcie dla emulatorów terminali m.in. emulatorów 3270 oraz 5250 firm Eicon, WRQ, IBM, NetManage, JollyGiant, Pericom jak również emulatorów telnet firm WRQ, IBM, Microsoft, Novell, 4. System musi umożliwiać scentralizowane zarządzanie SSO na poziomie pojedynczych użytkowników w strukturze usługi katalogowej, a także kontenerów usługi katalogowej. 5. System musi umożliwiać obsługę aplikacji dodawanych z wykorzystaniem graficznego kreatora, oraz z wykorzystaniem języka skryptowego. 6. System musi przechowywać dane logowania użytkowników w postaci zaszyfrowanej w usłudze katalogowej. 7. System musi posiadać opcjonalny cache chroniący dane logowania użytkownika na stacji roboczej, który pozwala na wykorzystanie rozwiązania również bez dostępu do usługi katalogowej 8. System musi umożliwiać wykorzystanie karty inteligentnej do przechowywania danych logowania oraz opcjonalne zaszyfrowanie lokalnego cache na stacji roboczej certyfikatem znajdującym się na karcie inteligentnej. 9. Dla współpracy z kartami kryptograficznymi system musi posiadać udokumentowane przez dostawcę systemu pojedynczego logowania wsparcie dla bibliotek PKCS#11 pochodzących od co najmniej 3 różnych producentów. 10. System musi posiadać możliwość wymuszenia obecności karty inteligentnej w czytniku kart dla działania klienta systemu pojedynczego logowania. 11. System musi posiadć możliwość wymuszenia podania przez użytkownika PIN do karty przed zalogowaniem do aplikacji (re-autentykacja). 12. System musi posiadać możliwość wymuszenia okresowej zmiany hasła użytkownika do wybranej aplikacji i jego automatyczne generowanie zgodnie ze zdefiniowanymi wymogami odnośnie siły hasła, nawet w przypadku jeżeli dana aplikacja w ogóle nie nakłada restrykcji na siłę hasła i nie wymaga jego okresowej zmiany. 13. System musi posiadać możliwość wymuszenia uwierzytelnienia użytkownika przed uruchomieniem aplikacji nawet w przypadku jeżeli aplikacja w ogóle nie wymaga uwierzytelnienia użytkownika. 14. System musi umożliwiać automatyczną obsługę następujących zdarzeń dla aplikacji:     1. logowanie     2. zmiana hasła     3. wymuszenie zmiany hasła po przekroczeniu czasu jego ważności. 15. System musi posiadać możliwość eksportu oraz importu danych logowania za pośrednictwem cyfrowo podpisanych oraz szyfrowanych plików XML. |  |  |  |  |

Tabela 14 Silne uwierzytelnianie oraz SSO



### Wymagania szczegółowe dla stosowanych produktów – sieć bezprzewodowa

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Sieć bezprzewodowa | Wymagania dotyczą:  WiFcnt.NET.CG | 1. Każde urządzenie musi umożliwiać zarządzanie docelowo przynajmniej 32 punktami dostępowymi sieci WiFi. 2. Urządzenie musi zarządzać centralnie wszystkimi punktami dostępowymi sieci WiFi. 3. Zestaw musi umożliwiać zbieranie informacji o poszczególnych stacjach roboczych podłączonych do punktów dostępowych sieci WiFi zarządzanych przez kontroler bezpośrednio z interfejsu WWW kontrolera (adres MAC, stan uwierzytelnienia stacji, przydzielony adres IP). 4. Zestaw musi umożliwiać uzyskanie informacji na temat obciążenia poszczególnych kanałów radiowych. 5. Kontroler musi posiadać następujące parametry sieciowe:    1. możliwość wdrożenia w warstwie 2 i 3 ISO/OSI,    2. wsparcie dla sieci VLAN w tym również trunk 802.1q    3. wbudowany serwer DHCP    4. obsługa SNMPv2, SNMPv3    5. Obsługa LAG    6. Obsługa Spanning tree oraz PVST+ 6. Kontroler musi posiadać następujące interfejsy sieciowe    1. Min. 4 porty 10/100/1000Base-T R4J5 7. Kontroler musi obsługiwać funkcję zarówno lokalnego, jak i centralnego przełączania ruchu 8. W dostarczonej wersji kontroler musi posiadać licencje umożliwiające obsługę    1. min. 20 AP pracujących w 802.11n z możliwością rozbudowy o co najmniej 10 kolejnych 9. Kontroler sieci WLAN musi obsługiwać nie mniej niż:    1. Metody szyfrowania i kontroli połączeń: WEP, TKIP WPA, WPA2, AES-CCMP, EAP, PEAP, TLS, TTLS,    2. Obsługa szyfrowania AES-CCM, TKIP i WEP    3. Certyfikaty cyfrowe X.509    4. Autoryzacja dostępu użytkowników:       1. Typy uwierzytelnienia: IEEE 802.1X (EAP,,PEAP,EAP-TLS,EAP-TTLS), captive portal i MAC       2. Możliwość utworzenia nie mniej niż 16 SSID na jednym punkcie dostępowym w przypadku stosowania bezprzewodowego punktu dostępowego z jednym modułem radiowym lub 32 SSID w przypadku dwóch modułów radiowych. Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania, oddzielnych vlan-ów       3. Uwierzytelnienie oraz autoryzacja musi być możliwa przy wykorzystaniu lokalnej bazy danych na kontrolerze oraz zewnętrznych serwerów uwierzytelniających. Kontroler musi wspierać co najmniej następujące serwery AAA: Radius, LDAP, Steel Belted Radius Server, Infranet Controller 10. Kontroler musi posiadać obsługę transmisji różnego typu danych w jednej sieci:     1. Integracja jednoczesnej transmisji danych i głosu     2. Obsługa QoS dla ruchu VoIP (dopuszcza się możliwość rozbudowy poprzez dokupienie licencji w przyszłości)     3. Obsługa fast roaming     4. Ograniczanie pasma 11. Kontroler musi posiadać funkcję sterowania funkcjami radiowymi do automatycznego zarządzania sygnałem oraz punktami dostępowymi:     1. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe     2. Stałe monitorowanie pasma     3. Rozkład ruchu pomiędzy różnymi punkami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma     4. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału     5. Wsparcie dla 802.11h     6. Integracja z systemami RFID 12. Kontroler musi posiadać funkcję zarządzać dostępem do sieci uwzględniając     1. Personalne listy kontroli dostępu     2. Szyfrowanie     3. Porę dnia/dzień tygodnia     4. Lokalizację, przy wykorzystaniu zewnętrznego systemu RTLS 13. Kontroler musi posiadać wbudowany system IDS/IPS o funkcjonalności:     1. Detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP).     2. Wykrywanie ataków DoS na sieć bezprzewodową     3. Identyfikacja podszywania się pod autoryzowane punkty dostępowe 14. Zarządzanie kontrolerem musi odbywać się poprzez co najmniej następujące metody: interfejs przeglądarki Web (http/ https) w zakresie podstawowych parametrów pracy, linia komend przez SSH/Telnet i dedykowany port konsoli 15. Wymagana zgodność z normami:     1. FCC Part 15 Class A   EN 55022 Class A   * 1. EN 55024   2. IEC/EN 60950   3. CE Marking |  |  |  |  |

Tabela 15 Kontroler sieci WiFi

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Sieć bezprzewodowa | Wymagania dotyczą:  WiF.NET.AP1  do  WiF.NET.AP18 | 1. Punkty dostępowe muszą być zasilane poprzez kabel sygnałowy Ethernet zgodnie ze standardem IEEE 802.3af 2. Punkty dostępowe muszą posiadać min. jeden moduł radiowy pracujący w standardzie 802.11a/n lub 802.11b/g/n 3. Punkty dostępowe muszą być zarządzane centralnie z poziomu kontrolerów 4. Interfejs radiowy musi mieć możliwość pracy w technologii MIMO 2x2 5. Punkty dostępowe muszą posiadać minimum dwie wewnętrzne anteny o mocy min. 21 dBm 6. Punkty dostępowe muszą być wyposażone w uchwyty umożliwiające ich montaż na suficie |  |  |  |  |

Tabela 16 Punkt dostępowy sieci WiFi

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Sieć bezprzewodowa | Wymagania dotyczą:  WiFrtr.NET.CG | 1. Urządzenie (Firewall/Gateway) musi być dostarczone jako dedykowane urządzenie sieciowe o wysokości maksimum 5U. 2. Urządzenie musi być wyposażone w co najmniej 512 MB pamięci RAM, pamięć Flash 1 GB oraz port konsoli. Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego firewalla z nośnika danych podłączonego do slotu USB na module kontrolnym. 3. System operacyjny firewalla musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł routingu IP, odpowiedzialny za ustalenie tras routingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. System operacyjny firewalla musi śledzić stan sesji użytkowników (stateful processing), tworzyć i zarządzać tablicą stanu sesji. Musi istnieć opcja przełączenia urządzenia w tryb pracy bez śledzenia stanu sesji użytkowników, jak również wyłączenia części ruchu ze śledzenia stanu sesji. 4. Urządzenie musi być wyposażone w nie mniej niż 2 wbudowane interfejsy Ethernet 10/100/1000 oraz 6 interfejsów 10/100 (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji). 5. Urządzenie musi być wyposażone w 1 slot na dodatkową kartę z modułami interfejsów. Urządzenie musi posiadać co najmniej następującej rodzaje kart z modułami interfejsów: Gigabit Ethernet (SFP). 6. Firewall musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż 10 strefami bezpieczeństwa z wydajnością nie mniejszą niż 225 Mb/s liczoną dla ruchu IMIX. 7. Firewall musi przetworzyć nie mniej niż 58 000 pakietów/sekundę (dla pakietów 64-bajtowych). Firewall musi obsłużyć nie mniej niż 28 000 równoległych sesji oraz zestawić nie mniej niż 1 450 nowych połączeń/sekundę. 8. Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN musi być realizowany sprzętowo. Firewall musi obsługiwać nie mniej niż 200 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 52 Mb/s. 9. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Firewall musi umożliwiać zdefiniowanie nie mniej niż 450 reguł polityki bezpieczeństwa. 10. Urządzenie musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF oraz BGP. Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 8 wirtualnych instancji. 11. Urządzenie musi obsługiwać co najmniej 32 sieci VLAN z tagowaniem 802.1Q. W celu zapobiegania zapętlania się ruchu w warstwie 2 firewall musi obsługiwać protokoły Spanning Tree (802.1D), Rapid STP (802.1W) oraz Multiple STP (802.1S). Urządzenie musi obsługiwać protokół LACP w celu agregowania fizycznych połączeń Ethernet. 12. Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków TCP i UDP. 13. Urządzenie musi posiadać tworzenia osobnych kolejek dla różnych klas ruchu. 14. Urządzenie musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach. 15. Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń. Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. 16. Zarządzanie urządzeniem musi odbywać się za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH. Firewall musi posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta (nie jest przedmiotem dostawy). |  |  |  |  |

Tabela 17 Styk z Internetem

#### Wymagania szczegółowe – zarządzanie tożsamością

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Zarządzanie tożsamością | Wymagania dotyczą:  DC.SRV.CG  DC.SRV.CZ | 1. System Zarządzania Tożsamością powinien posiadać wbudowane centralne repozytorium informacji o użytkownikach i zasobach oparte na katalogu 2. jest wymagane, aby było możliwe administrowanie centralne, ale z możliwością delegowania części uprawnień do administratorów poszczególnych jednostek lub usług 3. system winien zapewnić możliwość przypisania nadawania uprawnień dostępu dla jednej lub grupy osób 4. System zarządzania tożsamością powinien zapewniać możliwość działania systemu w środowisku heterogenicznym. Współpraca ta powinna być realizowana z użyciem standardowych dla źródeł danych protokołów dostępu oraz przy minimalnej ingerencji w mechanizmy działania źródła danych połączonego z systemem. 5. Musi posiadać wbudowaną zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, 6. Musi posiadać wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), 7. Musi posiadać tekstowy oraz graficzny interfejs użytkownika, 8. Musi umożliwiać obsługę systemów wieloprocesorowych do 64 procesorów, 9. Musi posiadać obsługę platform sprzętowych x64, 10. Musi posiadać możliwość zaadresowania maksymalnie 4TB pamięci RAM, 11. Musi posiadać możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, 12. Musi posiadać wsparcie dla protokołu IP w wersji 6 (IPv6), oraz protokołu Kerberos 13. Musi posiadać możliwość implementacji następujących komponentów i funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania): 14. podstawowych usług sieciowych: DNS, DHCP, SMTP 15. usług współdzielenia plików i drukarek, ze szczegółowym przypisywaniem uprawnień na poziomie udostępnionego katalogu (Odczyt, Modyfikacja, Pełna kontrola) oraz na poziomie plików (Odczyt, Zapis, Odczyt i Wykonanie, Modyfikacja, Pełna kontrola), dla użytkowników lokalnych i z usług katalogowych 16. usług katalogowych LDAP pozwalających na zarządzanie zasobami w sieci (użytkownicy, grupy, komputery, drukarki, udziały sieciowe), wraz z możliwościami wymuszania określonych ustawień dla użytkowników i komputerów 17. zdalną dystrybucję oprogramowania na stacje robocze, 18. centrum certyfikatów, obsługa klucza publicznego i prywatnego, szyfrowanie plików i folderów, szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi w obrębie sieci lokalnej, 19. usługę zdalnego dostępu do serwera z wykorzystaniem wirtualnych sieci prywatnych (VPN) 20. możliwość balansowania obciążeniem serwerów (NLB) oraz budowy klastrów niezawodnościowych (failover) do 32 węzłów, 21. platformę wirtualizacyjną umożliwiającą na uruchomienie dwóch wirtualnych maszyn z tym systemem operacyjnym na fizycznym serwerze 22. usługę udostępniania stron i aplikacji WWW wraz z platformą dla dynamicznych prekompilowanych stron internetowych 23. usługę terminalową - dostęp do pulpitu zdalnego poprzez dedykowanego klienta i stronę www, umożliwiającą pracę z dedykowanymi zainstalowanymi na serwerze aplikacjami poprzez zdalny pulpit serwera oraz z poziomu klienckiego systemu operacyjnego okno terminale ograniczone do wybranej aplikacji (podobnie jak w przypadku zainstalowanej lokalnie aplikacji) umożliwiając skojarzenie lokalnych plików klienta z aplikacją na serwerze, 24. usługę zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management), 25. usługę zarządzania polityką dostępu do sieci w oparciu o stan bezpieczeństwa klienta (zapora ogniowa, zainstalowane poprawki i sygnatury antywirusowe), 26. usługę serwera poprawek z możliwością automatycznej aktualizacji stacji roboczych i serwerów z wykorzystaniem protokołu HTTP/S 27. usługę zdalnego wdrażania systemów operacyjnych serwerowych i klienckich 28. zaawansowany język skryptowy umożliwiający zarządzanie wszystkimi komponentami i funkcjami serwera |  |  |  |  |

Tabela 18 Zarządzanie tożsamością

#### Dodatkowe licencje Microsoft

Należy dostarczyć następujące licencje :

1. Microsoft Windows 8 Pro – 150 szt.
2. Microsoft Office Standard 2013 – 150 szt.
3. Windows Server 2012 per User CAL – 400 szt.
4. Remote Desktop Services per User CAL – 240 szt.

Do systemu zarządzania tożsamością na 2 serwerach fizycznych oraz w/w licencji należy dostarczyć Software Assurance na okres co najmniej 5 lat biegnącego od momentu podpisania protokołu odbioru końcowego.



#### Wymagania szczegółowe – przełączniki SAN

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Przełączniki SAN | Wymagania dotyczą:  SAN1.SW.CG,  SAN2.SW.CG,  SAN1.SW.CZ,  SAN2.SW.CZ, | Przełącznik FC musi być wykonane w technologii FC 16 Gb/s i posiadać możliwość pracy portów FC z prędkościami 16, 8, 4, 2 Gb/s  Przełącznik FC musi być wyposażony w 24 aktywne porty FC  Przełącznik FC musi być wyposażony w co najmniej 22 wkładki SFP FC 8Gbit wielomodowe oraz 2 wkładki SFP FC 8Gbit jednomodowe zapewniające poprawną pracę na odległość minimum 10 km.  Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19 cali oraz zapewniać techniczną możliwość montażu w szafie 19 cali. Przełącznik musi być wyposażony w akcesoria umożliwiające montaż w szafie.  Przełącznik FC musi posiadać nadmiarowe i hotswapowe zasilacze i wentylatory.  Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN.  Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji oprogramowania wewnętrznego (firmware) w czasie pracy urządzenia.  Przełącznik musi posiadać wsparcie dla N\_Port ID Virtualization (NPIV), E\_Port, F\_Port, M\_Port.  Przełącznik FC musi posiadać mechanizmy zwiększające poziom bezpieczeństwa:   1. Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP 2. Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli Listy Kontroli Dostępu w sieci Fabric za pomocą protokołu DH-CHAP 3. Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów 4. Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2 5. Konta użytkowników definiowane w środowisku RADIUS lub LDAP 6. Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS   Przełącznik FC musi obsługiwać protokół SNMPv3  Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet.  Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz poprzez przeglądarkę internetową z interfejsem graficznym. |  |  |  |  |

Tabela 19 Przełączniki SAN



#### Wymagania szczegółowe – macierz o dostępie blokowym w Centrum Głównym

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Macierz dyskowa o dostępie blokowym, | Wymagania dotyczą:  SAN.STR.CG | Macierz musi posiadać pojemność surową co najmniej 68 TB  Przestrzeń musi być zbudowana w oparciu o dyski SSD (co najmniej 2szt.) o pojemności nie mniejszej 200GB, o dyski SAS/FC 10K (co najmniej 22szt.) o pojemności 900GB oraz dyski NL-SAS (co najmniej 12szt.) o pojemności 4TB.  Macierz musi umożliwiać rozbudowę do co najmniej 240 dysków (w konfiguracji dysków 2,5”) oraz do co najmniej 480 dysków (w konfiguracji dysków 2,5”) poprzez mechanizm klastrowania lub dodawania par kontrolerów.  Macierz musi posiadać pamięć cache co najmniej 16GB, po 8GB na kontroler z możliwością rozbudowy łącznie do 64GB poprzez mechanizm klastrowania lub dodawania par kontrolerów.  Macierz musi zabezpieczać dyski mechanizmami RAID 0, 1, 5, 6, 10.  Macierz musi posiadać funkcjonalność automatycznie odbudowywania danych z uszkodzonego dysku na wolnej przestrzeni SPARE.  Półki dyskowe muszą być podłączone do każdego z kontrolerów przez min. 2 redundantne połączenia FC lub SAS.  Min. 2 redundantne kontrolery macierzowe.  Wszystkie kontrolery muszą pracować w trybie active-active.  Oferowana konfiguracja musi zawierać mechanizm nie powodujący wyłączenia cache do zapisu w przypadku awarii kontrolera, przy zapewnieniu redundancji pamięci write-cache.  Każdy kontroler musi być wyposażony w minimum 4 porty FC 8Gbit, 2 porty Ethernet 1Gbit oraz 2 porty 10GbE.  Macierz musi posiadać możliwość wykonywania kopii danych typu klon mechanizmami macierzy (licencja na wykonywanie kopii pełnych musi być zawarta w oferowanej cenie macierzy)  Macierz musi posiadać możliwość wykonywania kopii danych typu snapshot mechanizmami macierzy. Minimalna liczba kopii nie może być mniejsza niż 100, w tym możliwość wykonywania kopii z kopii oraz promowania migawki do trybu RW  Kopie typu snapshot muszą być wykonywane w taki sposób by nie było konieczności rezerwacji miejsca dla zmieniających się danych.  Macierz musi posiadać funkcjonalność LUN masking, LUN mapping  Macierz musi posiadać możliwość udostępniania wolumenów o większej pojemności niż aktualnie zaalokowana dla tego wolumenu. Funkcjonalność musi być oferowana dla całej pojemności macierzy.  Macierz musi posiadać możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy tymi samymi typami macierzy dyskowych. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach. Z macierzą dostarczone muszą być licencje na replikacje danych między macierzami w Centrum Głównym a Zapasowym.  Replikacja pomiędzy macierzami musi zapewniać realizację planu Disaster Recovery, tzn. w przypadku całkowitego uszkodzenia jednej macierzy, jest możliwość uruchomienia zasobów na drugiej macierzy w sposób zautomatyzowany z zapewnieniem integracji z natywnymi mechanizmami dostarczanego oprogramowania wirtualizującego.  Macierz musi mieć możliwość wykonania migracji wolumenów logicznych wewnątrz macierzy, bez zatrzymywania aplikacji korzystającej z tych wolumenów. Zasoby źródłowe podlegające migracji oraz zasoby do których są migrowane mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach.  Macierz musi posiadać narzędzia do monitorowania i planowania wydajności oraz pojemności macierzy. Przechowywane historii wydajności musi być wykonywane mechanizmami macierzy.  Macierz musi zapewniać techniczną możliwość montażu w szafie 19 cali oraz musi być wyposażony w akcesoria umożliwiające montaż w szafie.  Macierz musi posiadać możliwość zabezpieczenia danych znajdujących się w pamięci cache w przypadku awarii zasilania na min. 3 dni  Macierz musi pozwalać na wymianę w trakcie pracy następujących elementów: dysków, kontrolerów, zasilaczy.  Macierz musi posiadać oprogramowanie do zarządzania zarówno przez interfejs graficzny GUI oraz tekstowy CLI. Możliwość zarządzania zdalnego macierzą przez tzw. „command line” z wykorzystniem protokołu SSH.  Macierz musi umożliwiać rozbudowę o dwa redundantne moduły udostępniające przestrzeń dyskową z wykorzystaniem protokołu SMB i NFS.  Z macierzą musi zostać dostarczone oprogramowanie zarządzające wielościeżkowością połączeń MPIO dla wszystkich podłączanych do macierzy serwerów. |  |  |  |  |

Tabela 20 Macierz dyskowa o dostępie blokowym w Centrum Głównym

#### Wymagania szczegółowe – macierz o dostępie blokowym w Centrum Zapasowym

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Macierz dyskowa o dostępie blokowym, | Wymagania dotyczą:  SAN.STR.CZ | Macierz musi posiadać pojemność surową co najmniej 48 TB  Przestrzeń musi być zbudowana w oparciu o dyski NL-SAS (co najmniej 12szt.) o pojemności 4TB.  Macierz musi umożliwiać rozbudowę do co najmniej 240 dysków (w konfiguracji dysków 2,5”) oraz do co najmniej 480 dysków (w konfiguracji dysków 2,5”) poprzez mechanizm klastrowania lub dodawania par kontrolerów.  Macierz musi posiadać pamięć cache co najmniej 16GB, po 8GB na kontroler z możliwością rozbudowy łącznie do 64GB poprzez mechanizm klastrowania lub dodawania par kontrolerów.  Macierz musi zabezpieczać dyski mechanizmami RAID 0, 1, 5, 6, 10.  Macierz musi posiadać funkcjonalność automatycznie odbudowywania danych z uszkodzonego dysku na wolnej przestrzeni SPARE.  Półki dyskowe muszą być podłączone do każdego z kontrolerów przez min. 2 redundantne połączenia FC lub SAS.  Min. 2 redundantne kontrolery macierzowe.  Wszystkie kontrolery muszą pracować w trybie active-active.  Oferowana konfiguracja musi zawierać mechanizm nie powodujący wyłączenia cache do zapisu w przypadku awarii kontrolera, przy zapewnieniu redundancji pamięci write-cache.  Każdy kontroler musi być wyposażony w minimum 4 porty FC 8Gbit, 2 porty Ethernet 1Gbit oraz 2 porty 10GbE.  Macierz musi posiadać możliwość wykonywania kopii danych typu klon mechanizmami macierzy (licencja na wykonywanie kopii pełnych musi być zawarta w oferowanej cenie macierzy)  Macierz musi posiadać możliwość wykonywania kopii danych typu snapshot mechanizmami macierzy. Minimalna liczba kopii nie może być mniejsza niż 100, w tym możliwość wykonywania kopii z kopii oraz promowania migawki do trybu RW  Kopie typu snapshot muszą być wykonywane w taki sposób by nie było konieczności rezerwacji miejsca dla zmieniających się danych.  Macierz musi posiadać funkcjonalność LUN masking, LUN mapping  Macierz musi posiadać możliwość udostępniania wolumenów o większej pojemności niż aktualnie zaalokowana dla tego wolumenu. Funkcjonalność musi być oferowana dla całej pojemności macierzy.  Macierz musi posiadać możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy tymi samymi typami macierzy dyskowych. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach. Z macierzą dostarczone muszą być licencje na replikacje danych między macierzami w Centrum Głównym a Zapasowym.  Replikacja pomiędzy macierzami musi zapewniać realizację planu Disaster Recovery, tzn. w przypadku całkowitego uszkodzenia jednej macierzy, jest możliwość uruchomienia zasobów na drugiej macierzy w sposób zautomatyzowany z zapewnieniem integracji z natywnymi mechanizmami dostarczanego oprogramowania wirtualizującego.  Macierz musi mieć możliwość wykonania migracji wolumenów logicznych wewnątrz macierzy, bez zatrzymywania aplikacji korzystającej z tych wolumenów. Zasoby źródłowe podlegające migracji oraz zasoby do których są migrowane mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach.  Macierz musi posiadać narzędzia do monitorowania i planowania wydajności oraz pojemności macierzy. Przechowywane historii wydajności musi być wykonywane mechanizmami macierzy.  Macierz musi zapewniać techniczną możliwość montażu w szafie 19 cali oraz musi być wyposażony w akcesoria umożliwiające montaż w szafie.  Macierz musi posiadać możliwość zabezpieczenia danych znajdujących się w pamięci cache w przypadku awarii zasilania na min. 3 dni  Macierz musi pozwalać na wymianę w trakcie pracy następujących elementów: dysków, kontrolerów, zasilaczy.  Macierz musi posiadać oprogramowanie do zarządzania zarówno przez interfejs graficzny GUI oraz tekstowy CLI. Możliwość zarządzania zdalnego macierzą przez tzw. „command line” z wykorzystniem protokołu SSH.  Macierz musi umożliwiać rozbudowę o dwa redundantne moduły udostepniające przestrzeń dyskową z wykorzystaniem protokołu SMB i NFS.  Z macierzą musi zostać dostarczone oprogramowanie zarządzające wielościeżkowością połączeń MPIO dla wszystkich podłączanych do macierzy serwerów. |  |  |  |  |

Tabela 21 Macierz dyskowa o dostępie blokowym w Centrum Zapasowym

#### Wymagania szczegółowe – moduły dostępu plikowego do macierzy blokowej

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Moduły dostępu plikowego do macierzy blokowej | Wymagania dotyczą:  NAS.STR.CG,  NAS.STR.CZ | Macierz musi posiadać dwa redundantne moduły udostepniające przestrzeń dyskową z wykorzystaniem protokołu SMB i NFS.  Moduł musi posiadać co najmniej 2 porty 1GbE, 2 porty 10GbE, 2 porty 8Gb FC.  Moduły muszą zapewniać dostęp do danych z wykorzystaniem protokołu SMB i NFS.  Moduły muszą posiadać możliwość integracji z Active Directory.  Rozwiązanie macierzy i modułów musi pochodzić od jednego producenta i być oferowane w ramach jednej rodziny produktowej.  Moduły muszą posiadać redundantne zasilacze.  Moduły muszą zapewniać techniczną możliwość montażu w szafie 19” oraz musi być wyposażony w akcesoria umożliwiające montaż w szafie. |  |  |  |  |

Tabela 22 Moduły dostępu plikowego do macierzy blokowej



#### Wymagania szczegółowe – system tworzenia kopii zapasowych

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| System tworzenia kopii zapasowych | Wymagania dotyczą:  BCK.SYS.CG,  BCK.SYS.CZ | Oprogramowanie systemu tworzenia kopii zapasowych musi zapewnić możliwość wykonywania kopii bezpieczeństwa w dostarczonym środowisku  Oprogramowanie musi umożliwiać wykonywanie backupów dla systemów: Linux RHEL, SUSE, Mac oraz Windows  Do przechowywania danych wykorzystywane muszą być bezobsługowe biblioteki taśmowe oraz lokalne dyski  System musi zapewnić możliwość odtworzenia danych w przypadku ich utraty oraz testowania procedur związanych z odtwarzaniem danych.  System musi zapewnić możliwość tworzenia kopii zapasowych zarówno na dyski jak i na napędy taśmowe.  Aktualne kopie muszą być przechowywane na dyskach.  Dostarczone licencje muszą zapewnić możliwość wykonywania kopii bezpieczeństwa dla wszystkich serwerów dostarczonych w ramach projektu.  Dostarczone oprogramowanie musi zapewnić możliwość wykorzystania wszystkich dostarczonych napędów przez oba serwery systemu tworzenia kopii bezpieczeństwa  Dostarczone oprogramowanie musi zapewnić możliwość zapisywania danych na wewnętrznych macierzach serwerów systemu kopii zapasowej  Dostarczone oprogramowanie musi zapewnić możliwość replikacji deduplikowanych backupów między serwerami kopii zapasowych  Dostarczone oprogramowanie do kopii zapasowych musi chronić środowiska fizyczne i wirtualne.  Dostarczone oprogramowanie musi pozwalać odzyskiwać dane, systemy operacyjne i aplikacje od pojedynczych elementów po serwery.  Dostarczone oprogramowanie musi umożliwiać funkcjonalność deduplikacji i archiwizacji danych w celu ograniczania rozmiarów i kosztów pamięci masowej. Dostarczone oprogramowanie do kopii zapasowych musi oferować zaawansowane funkcje tworzenia kopii zapasowych i odzyskiwania danych w środowiskach VMware i Hyper-V oraz systemach Windows, Linux i Mac. Dla VMware musi integrować się z VMware Data Protection APIs oferując kopie przyrostowe z wykorzystaniem CBT (Change Block Tracking) a dla Hyper-V oferować wykonywanie kopii przyrostowych i różnicowych.  Dostarczone oprogramowanie do kopii zapasowych musi posiadać funkcje odtwarzania danych po awarii od zera umożliwiając przywracanie kopii zapasowych całych serwerów na innych platformach sprzętowych lub przywracać w maszyny wirtualne w celu szybkiego odtwarzania danych.  Dostarczone oprogramowanie do kopii zapasowych musi umożliwiać odtwarzanie danych aplikacji fizycznych i wirtualnych na dowolnym poziomie szczegółowości dla programów MS Exchange, Active Directory, SharePoint i SQL Server w środowiskach wirtualnych (np. pojedyncze wiadomości e-mail, dokumenty programu SharePoint, obiekty usług Active Directory i bazy danych SQL Server).  Licencje powinny obejmować wykonywanie kopii zapasowych na całe dostarczone środowisko Systemu Wirtualizacji Serwerowej i wirtualnych maszyn oraz aplikacji na nich pracujących, oraz systemu zarządzania tożsamością IDM. |  |  |  |  |

Tabela 23 System tworzenia kopii zapasowych



#### Wymagania szczegółowe – biblioteka taśmowa

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Biblioteka taśmowa, | Wymagania dotyczą:  BCK.TLB.CG,  BCK.TLB.CZ | Napędy taśmowe:   1. Biblioteka powinna być wyposażona w minimum 2 napędy taśmowe LTO 6 z natywnym interfejsem Fibre Channel 8 Gb/s 2. Biblioteka powinna umożliwiać wymianę napędów bez przerywania pracy (napędy typu „hot swap"). 3. Minimalna pojemność pojedynczej taśmy bez kompresji danych to 2,5 TB.   Interfejs i sterowanie robotyką:   1. Każdy zainstalowany napęd taśmowy musi posiadać natywny interfejs Fibre Chanel 8Gb/s (stosowanie konwerterów SCSI-to-Fibre Channel jest niedopuszczane). 2. Dane sterujące biblioteką muszą być przesyłane w paśmie Fibre Channel napędów taśmowych z prędkością 8 Gbit/s. Brak dodatkowego łącza do przesyłania danych sterujących biblioteką taśmową.   Parametry techniczne:   1. Dopuszczalna temperatura pracy 10 do 45 stopni Celsjusza, 2. Dopuszczalny zakres wilgotności pracy urządzenia 10 do 80%.   Zarządzanie:   1. Biblioteka musi być wyposażona w moduł zdalnego zarządzania 2. Biblioteka musi udostępniać funkcję monitorowania stanu napędów. 3. Biblioteka musi udostępniać możliwość zarządzania przez przeglądarkę WWW. 4. Biblioteka taśmowa powinna mieć również możliwość zdalnego monitorowania stanu urządzenia i wychwytywania błędów. 5. Biblioteka powinna umożliwiać wsparcie dla:    1. posiadać wbudowanego agenta SNMP,    2. posiadać możliwość wysyłania alertów o różnym stopniu ważności na różne adresy email,    3. posiadać możliwość definiowania grup użytkowników z różnymi prawami dostępu do biblioteki. 6. Biblioteka taśmowa musi być wyposażona w prosty w obsłudze i czytelny wyświetlacz/panel sterowania udostępniający:    1. podstawowe funkcje zarządzające,    2. zajętość slotów przez taśmy,    3. liczbę taśm zamontowanych w napędach.   Sloty na taśmy:   1. Biblioteka musi być dostarczona w konfiguracji sprzętowej wraz z zestawem niezbędnych licencji pozwalających na użytkowanie minimum 48 kieszeni (ang. slots) na nośniki. 2. Biblioteka musi pozwalać na zdefiniowanie co najmniej 3 mail slots, służących do importu i exportu nośników.   Możliwości rozbudowy:   1. Biblioteka musi mieć możliwość rozbudowy systemu do co najmniej 4 napędów taśmowych.   Wraz z urządzeniem musi być dostarczony zestaw do montażu biblioteki taśmowej w szafie RACK 19 cali  Wyposażenie dodatkowe:   1. Czytnik kodów kreskowych. 2. Biblioteka powinna być wyposażona w redundantne zasilacze typu Hot Swap. 3. Wraz z biblioteką wymaga się dostarczenia:    1. 50 sztuk taśm LTO 6    2. 2 sztuki taśm czyszczących LTO. |  |  |  |  |

Tabela 24 Biblioteka taśmowa



#### Wymagania szczegółowe – terminalowe środowisko pracy użytkownika

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Terminalowe środowisko pracy użytkownika | Wymagania dotyczą:  WTSx.VRT.SCO | Oprogramowanie dostarczające pulpit roboczy będzie zapewniać   1. Równoważenie obciążenia maszyn hostujących środowisko terminalowe 2. Zapewniać wysoką dostępność środowiska terminalowego w przypadku awarii elementów infrastruktury 3. Integracje ze środowiskiem domenowym 4. Dostarczać interfejs umożliwiający scentralizowane zarządzanie farmą serwerów terminalowych 5. Musi wspierać następujące rozwiązania wirtulizacyjne: MS Hyper-V i VMware vSphere 6. Musi zapewniać integracje z usługami katalogowymi Active Directory 7. Musi umożliwiać przypisanie użytkowników lub grup użytkowników do konkretnej aplikacji 8. Musi umożliwiać współdzielenie serwera terminalowego przez wielu użytkowników 9. Musi umożliwiać uwierzytelnianie się użytkowników do środowiska serwerów terminalowych z wykorzystaniem kart inteligentnych 10. Musi umożliwiać bezpieczne połączenie z serwerem bramy z wykorzystaniem tunelowania SSL 11. Musi umożliwiać bezpieczne połączenie z serwerem bramy z wykorzystaniem tunelowania SSL 12. Musi umożliwiać równoważenie obciążenia pomiędzy serwerami terminalowami i funkcjonalność brokera sesji 13. Musi umożliwiać dostęp do zdalnego pulpitu i aplikacji z urządzenia końcowego z systemem operacyjnym Windows, Linux oraz MacOS. Rozwiązanie musi umożliwiać publikację strony web z udostępnianymi aplikacjami dla zalogowanych użytkowników. |  |  |  |  |

Tabela 25 Terminalowe środowisko pracy użytkownika



#### Wymagania szczegółowe – system zarządzania urządzeniami końcowymi

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| System zarządzania urządzeniami końcowymi | Wymagania dotyczą:  WDS.VRT.SCO | 1. System musi umożliwiać: 2. Zarządzanie oprogramowaniem – zarządzanie patch’ami, upgradem systemu operacyjnego, instalacja poprawek 3. Integracja z usługami katalogowymi 4. Organizowanie urządzeń/systemów w grupy 5. Kontrole zainstalowanego oprogramowania 6. Raportowanie 7. Automatyczną reinstalację końcówek |  |  |  |  |

Tabela 26 System zarządzania urządzeniami końcowymi

#### Wymagania szczegółowe – serwer wydruku

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Serwer wydruku | Wymagania dotyczą:  PSx.VRT.SCO | - Serwer wydruku musi obsługiwać pule drukowania tak by wysłany do druku  dokument drukował się na najbliższej dostępnej drukarce.  - Serwer musi umożliwiać wysyłanie do druku dokumentów z różnych systemów operacyjnych (Windows, UNIX, Linux)  - Serwer wydruku powinien integrować się z usługami katalogowymi  - Serwer musi mieć możliwość zarządzanie przez www |  |  |  |  |

Tabela 27 Serwer wydruków



#### Wymagania szczegółowe - System zabudowy infrastruktury IT z szafami typu rack 19 cali

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| System zabudowy infrastruktury IT z szafami typu rack 19 cali z podsystemami dystrybucji zasilania PDU („Power Distribution Unit”), dla infrastruktury IT o dużej koncentracji mocy wraz z kontrolą dostępu („Access Control”). | Wymagania dotyczą:  RCK.INF.CG | Maksymalna wysokość zestawu: 2200 [mm] |  |  |  |  |
| Maksymalna długość zestawu: 1200 [mm] |
| Maksymalna szerokość zestawu: 1800 [mm] |
| Minimalna dostępna przestrzeń dla montażu infrastruktury IT w standardzie rack 19 cali: 126 U |
| System kontroli przepływu powietrza („Airflow Management”)na zasadzie rozdzielenia stref zimnych i ciepłych (tzw. „Row cooling”) |
| Rodzaj strefy zamkniętej („Hot/Cold Aisle”): Zimna |
| Szerokość strefy zamkniętej: 120 [mm] |
| Współpraca z podniesioną podłogą techniczną |
| 2 sztuki PDU dla każdego stelażu rack 19 cali: |
| PDU trójfazowe pionowe, zamontowane z tyłu stelażu nie zasłaniające torów wentylacyjnych sprzętu, o wysokości całkowitej dedykowanej do montażu w szafie 42U. |
| Rozdział mocy PDU na 6 sekcji jednofazowych zabezpieczonych wkładkami 16A w klasie C |  |  |  |  |
| Kontrolki obecności napięcia dla każdej sekcji PDU z możliwością niezależnego wyłączenia każdej sekcji |
| 24 sztuki gniazd CEE7/5,heavy duty lub gniazd C13, 16A dla każdego PDU |
| System kontroli dostępu (SKD) w postaci sterowanego i monitorowanego elektrozaczepu. |
| Wydzielenie dostępu dla każdej strony pojedynczego stelażu 19 cali oraz całego systemu zabudowy |
| Dopuszczalna moc dla zainstalowanej infrastruktury IT: min. 6 [kW] dla pojedynczego stelażu rack. |

Tabela 28 System zabudowy infrastruktury IT w Centrum Głównym z szafami typu rack 19 cali

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| System zabudowy infrastruktury IT z szafami typu rack 19 cali z podsystemami dystrybucji zasilania PDU („Power Distribution Unit”), dla infrastruktury IT o dużej koncentracji mocy wraz z kontrolą dostępu („Access Control”). | Wymagania dotyczą:  RCK.INF.CZ | Maksymalna wysokość zestawu: 2200 [mm] |  |  |  |  |
| Maksymalna długość zestawu: 1200 [mm] |
| Maksymalna szerokość zestawu: 1200 [mm] |
| Minimalna dostępna przestrzeń dla montażu infrastruktury IT w standardzie rack 19 cali: 84 U |
| System kontroli przepływu powietrza („Airflow Management”)na zasadzie rozdzielenia stref zimnych i ciepłych (tzw. „Row cooling”) |
| Rodzaj strefy zamkniętej („Hot/Cold Aisle”): Zimna |
| Szerokość strefy zamkniętej: 120 [mm] |
| Współpraca z podniesioną podłogą techniczną |
| 2 sztuki PDU dla każdego stelażu rack 19 cali: |
| PDU trójfazowe pionowe, zamontowane z tyłu stelażu nie zasłaniające torów wentylacyjnych sprzętu, o wysokości całkowitej dedykowanej do montażu w szafie 42U. |
| Rozdział mocy PDU na 6 sekcji jednofazowych zabezpieczonych wkładkami 16A w klasie C |
| Kontrolki obecności napięcia dla każdej sekcji PDU z możliwością niezależnego wyłączenia każdej sekcji |
| 24 sztuki gniazd CEE7/5,heavy duty lub gniazd C13, 16A dla każdego PDU |
| System kontroli dostępu (SKD) w postaci sterowanego i monitorowanego elektrozaczepu. |
| Wydzielenie dostępu dla każdej strony pojedynczego stelażu 19 cali oraz całego systemu zabudowy |
| Dopuszczalna moc dla zainstalowanej infrastruktury IT: min. 6 [kW] dla pojedynczego stelażu rack. |

Tabela 29 System zabudowy infrastruktury IT w Centrum Zapasowym z szafami typu rack 19 cali

#### Wymagania szczegółowe - System KVM

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| System KVM | Wymagania dotyczą:  KVM.INF.CG | Rozwiązanie musi posiadać klawiaturę, mysz lub touchpad oraz monitor w postaci wysuwanego panelu o wysokości maksymalnie 1U z możliwością montażu w standardowej szafie rack  Monitor w rozmiarze minimum 17” musi obsługiwać minimalną rodzielczość 1280 x 1024 przy 75Hz (dla proporcji 5:4 i 4:3) lub 1440 x 900 przy 75Hz (dla proporcji 16:10 i 16:9)  Moduł przełączający KVM musi umożlwiać kaskadowe podłączanie kolejnych modułów KVM  Dostarczone moduły KVM muszą umożliwiać podłączenie liniowo lub kaskadowo co najmniej 24 serwery z wykorzystaniem pojedynczego kabla (od modułu do serwera) z możliwością rozbudowy do co najmniej 128 serwerów.  Moduł przełączający KVM musi umożlwiać różne opcje konwersji sygnałów KVM |  |  |  |  |

Tabela 30 System KVM w Centrum Głównym

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| System KVM | Wymagania dotyczą:  KVM.INF.CZ | Rozwiązanie musi posiadać klawiaturę, mysz lub touchpad oraz monitor w postaci wysuwanego panelu o wysokości maksymalnie 1U z możliwością montażu w standardowej szafie rack  Monitor w rozmiarze minimum 17” musi obsługiwać minimalną rodzielczość 1280 x 1024 przy 75Hz (dla proporcji 5:4 i 4:3) lub 1440 x 900 przy 75Hz (dla proporcji 16:10 i 16:9)  Moduł przełączający KVM musi umożlwiać kaskadowe podłączanie kolejnych modułów KVM  Dostarczone moduły KVM muszą umożliwiać podłączenie liniowo lub kaskadowo co najmniej 8 serwerów z wykorzystaniem pojedynczego kabla (od modułu do serwera) z możliwością rozbudowy do co najmniej 128 serwerów.  Moduł przełączający KVM musi umożlwiać różne opcje konwersji sygnałów KVM |  |  |  |  |

Tabela 31 System KVM w Centrum Zapasowym



#### Wymagania szczegółowe – serwer systemu wirtualizacji serwerowej w centrum głównym – 5 sztuk

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Serwer systemu wirtualizacji serwerowej | Wymagania dotycząc:  SCOx.SRV.CG | Serwer musi posiadać obudowę typu RACK.  Serwer musi posiadać dwa dziesięciordzeniowe procesory taktowane zegarem co najmniej 2,5 GHz. Serwer musi posiadać co najmniej 256 GB pamięci RAM min. 1866 MHz oraz możliwość instalacji co najmniej 768 GB pamięci.  Serwer musi posiadać co najmniej 2 dyski o pojemności co najmniej 300GB i prędkości obrotowej 10000 rpm z możliwością rozbudowy do 16 dysków.  Serwer musi posiadać kontroler dyskowy umożliwiający utworzenie RAID 0, 1, 5, 10 z pamięcią 1GB cache podtrzymywanego bateryjnie lub flash-backed  Serwer musi posiadać co najmniej 1 slot PCI-E 3.0 x16 (elektrycznie), oraz 4 sloty PCI-E 3.0 x8 (elektrycznie)  Serwer musi posiadać co najmniej 6 zewnętrznych portów USB, 2 porty VGA (przód,tył), oraz 2 wewnętrzne porty USB lub SD  Serwer musi posiadać minimum 4 porty Ethernet typu 10/100/1000, 2 porty 10Gb Ethernet na płycie głównej serwera dostępnych z poziomu systemu operacyjnego oraz jeden dedykowany port Ethernet dla zdalnego zarządzania.  Serwer musi posiadać kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzanie włącznie z przejęciem zdalnym konsoli graficznej oraz zdalnego podłączenia napędów na poziomie sprzętowym  Serwer musi posiadać wsparcie dla protokołu IPMI w wersji 2.0  Serwer musi posiadać minimum dwa porty FC 8Gb/s.  Serwer musi posiadać nadmiarowe i hotswapowe wentylatory i zasilacze o mocy co najmniej 750W  Serwer musi posiadać kartę VGA  Serwer musi posiadać wysokość maksymalnie 2U do instalacji w standardowej szafie RACK 19 cali. Obudowa musi być dostarczona wraz z wszystkimi elementami mocującymi  Wraz z każdym z serwerów należy dostarczyć system operacyjny zgodny z dostarczonymi serwerami oraz oprogramowaniem do tworzenia kopii zapasowych |  |  |  |  |

Tabela 32 Serwer wirtualizacji serwerowej w centrum głównym

#### Wymagania szczegółowe – serwer systemu wirtualizacji serwerowej w centrum zapasowym – 3 sztuki.

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Serwer systemu wirtualizacji serwerowej | Wymagania dotycząc:  SCOx.SRV.CZ | Serwer musi posiadać obudowę typu RACK.  Serwer musi posiadać dwa dwunastordzeniowe procesory taktowane zegarem co najmniej 2,4 GHz. Serwer musi posiadać co najmniej 384 GB pamięci RAM min. 1866 MHz oraz możliwość instalacji co najmniej 768 GB pamięci.  Serwer musi posiadać co najmniej 2 dyski o pojemności co najmniej 300GB i prędkości obrotowej 10000 rpm z możliwością rozbudowy do 16 dysków.  Serwer musi posiadać kontroler dyskowy umożliwiający utworzenie RAID 0, 1, 5, 10 z pamięcią 1GB cache podtrzymywanego bateryjnie lub flash-backed  Serwer musi posiadać co najmniej 1 slot PCI-E 3.0 x16 (elektrycznie), oraz 4 sloty PCI-E 3.0 x8 (elektrycznie)  Serwer musi posiadać co najmniej 6 zewnętrznych portów USB, 2 porty VGA (przód,tył), oraz 2 wewnętrzne porty USB lub SD  Serwer musi posiadać minimum 4 porty Ethernet typu 10/100/1000, 2 porty 10Gb Ethernet na płycie głównej serwera dostępnych z poziomu systemu operacyjnego oraz jeden dedykowany port Ethernet dla zdalnego zarządzania.  Serwer musi posiadać kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzanie włącznie z przejęciem zdalnym konsoli graficznej oraz zdalnego podłączenia napędów na poziomie sprzętowym  Serwer musi posiadać wsparcie dla protokołu IPMI w wersji 2.0  Serwer musi posiadać minimum dwa porty FC 8Gb/s.  Serwer musi posiadać nadmiarowe i hotswapowe wentylatory i zasilacze o mocy co najmniej 900W  Serwer musi posiadać kartę VGA  Serwer musi posiadać wysokość maksymalnie 2U do instalacji w standardowej szafie RACK 19 cali. Obudowa musi być dostarczona wraz z wszystkimi elementami mocującymi  Wraz z każdym z serwerów należy dostarczyć system operacyjny zgodny z dostarczonymi serwerami oraz oprogramowaniem do tworzenia kopii zapasowych |  |  |  |  |

Tabela 33 Serwer wirtualizacji serwerowej w centrum zapasowym



#### Wymagania szczegółowe – serwer kontrolera domeny Active Directory

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Serwer kontrolera domeny | Wymagania dotycząc:  DC.SRV.CG  DC.SRV.CZ | Serwer musi posiadać obudowę typu RACK.  Serwer musi posiadać jeden czterordzeniowy procesor taktowany zegarem co najmniej 2,4 GHz. Serwer musi posiadać co najmniej 8GB pamięci RAM min. 1333 MHz oraz możliwość instalacji co najmniej 768 GB pamięci.  Serwer musi posiadać co najmniej 2 dyski o pojemności co najmniej 300GB i prędkości obrotowej 10000 rpm z możliwością rozbudowy do 8 dysków.  Serwer musi posiadać kontroler dyskowy umożliwiający utworzenie RAID 0, 1  Serwer musi posiadać co najmniej 1 slot PCI-E 3.0 x16 (elektrycznie), oraz 1 slot PCI-E 3.0 x8 (elektrycznie)  Serwer musi posiadać co najmniej 6 zewnętrznych portów USB, 2 porty VGA (przód,tył), oraz 1 wewnętrzny port USB lub SD  Serwer musi posiadać minimum 4 porty Ethernet typu 10/100/1000 na płycie głównej serwera dostępnych z poziomu systemu operacyjnego oraz jeden dedykowany port Ethernet dla zdalnego zarządzania.  Serwer musi posiadać kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzanie włącznie z przejęciem zdalnym konsoli graficznej oraz zdalnego podłączenia napędów na poziomie sprzętowym  Serwer musi posiadać wsparcie dla protokołu IPMI w wersji 2.0  Serwer musi posiadać nadmiarowe i hotswapowe wentylatory i zasilacze o mocy co najmniej 500W  Serwer musi posiadać kartę VGA  Serwer musi posiadać wysokość maksymalnie 1U do instalacji w standardowej szafie RACK 19 cali. Obudowa musi być dostarczona wraz z wszystkimi elementami mocującymi  Wraz z każdym z serwerów należy dostarczyć system operacyjny zgodny z dostarczonymi serwerami oraz oprogramowaniem do tworzenia kopii zapasowych |  |  |  |  |

Tabela 34 Serwer kontrolera domeny Active Directory



#### Wymagania szczegółowe – serwer monitoringu

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Serwer monitoringu | Wymagania dotycząc:  MON.SRV.CG  MON.SRV.CZ | Serwer musi posiadać obudowę typu RACK.  Serwer musi posiadać jeden czterordzeniowy procesor taktowany zegarem co najmniej 2,4 GHz. Serwer musi posiadać co najmniej 8GB pamięci RAM min. 1333 MHz oraz możliwość instalacji co najmniej 768 GB pamięci.  Serwer musi posiadać co najmniej 2 dyski o pojemności co najmniej 300GB i prędkości obrotowej 10000 rpm z możliwością rozbudowy do 8 dysków.  Serwer musi posiadać kontroler dyskowy umożliwiający utworzenie RAID 0, 1  Serwer musi posiadać co najmniej 1 slot PCI-E 3.0 x16 (elektrycznie), oraz 1 slot PCI-E 3.0 x8 (elektrycznie)  Serwer musi posiadać co najmniej 6 zewnętrznych portów USB, 2 porty VGA (przód,tył), oraz 1 wewnętrzny port USB lub SD  Serwer musi posiadać minimum 4 porty Ethernet typu 10/100/1000 na płycie głównej serwera dostępnych z poziomu systemu operacyjnego oraz jeden dedykowany port Ethernet dla zdalnego zarządzania.  Serwer musi posiadać kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzanie włącznie z przejęciem zdalnym konsoli graficznej oraz zdalnego podłączenia napędów na poziomie sprzętowym  Serwer musi posiadać wsparcie dla protokołu IPMI w wersji 2.0  Serwer musi posiadać nadmiarowe i hotswapowe wentylatory i zasilacze o mocy co najmniej 500W  Serwer musi posiadać kartę VGA  Serwer musi posiadać wysokość maksymalnie 1U do instalacji w standardowej szafie RACK 19 cali. Obudowa musi być dostarczona wraz z wszystkimi elementami mocującymi  Wraz z każdym z serwerów należy dostarczyć system operacyjny zgodny z dostarczonymi serwerami oraz oprogramowaniem do tworzenia kopii zapasowych |  |  |  |  |

Tabela 35 Serwer monitoringu



#### Wymagania szczegółowe - serwery systemu tworzenia kopii zapasowych

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Serwer systemu tworzenia kopii zapasowych | Wymagania dotyczączą:  BCK.SRV.CG,  BCK.SRV.CZ | Serwer musi posiadać obudowę typu RACK. Serwer musi posiadać dwa ośmiordzeniowe procesory taktowane zegarem co najmniej 2,3 GHz. Serwer musi posiadać co najmniej 32 GB pamięci RAM min. 1333 MHz oraz możliwość instalacji co najmniej 384 GB pamięci.  Serwer musi posiadać co najmniej 4 sloty PCI-E 3.0 x8 (elektrycznie).  Serwer musi posiadać co najmniej 12 dysków o pojemności co najmniej 4TB i prędkości obrotowej 7200 rpm  Serwer musi posiadać kontroler dyskowy umożliwiający utworzenie RAID 0, 1, 5, 10 z pamięcią 1GB cache podtrzymywanego bateryjnie lub flash-backed  Serwer musi posiadać co najmniej 6 zewnętrznych portów USB, 1 port VGA oraz 2 wewnętrzne porty USB lub SD  Serwer musi posiadać minimum dwa porty FC 8Gb/s.  Serwer musi posiadać minimum 4 porty Ethernet typu 10/100/1000, 2 porty 10Gb Ethernet na płycie głównej serwera dostępnych z poziomu systemu operacyjnego oraz jeden dedykowany port Ethernet dla zdalnego zarządzania.  Serwer musi posiadać kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzanie włącznie z przejęciem zdalnym konsoli graficznej oraz zdalnego podłączenia napędów na poziomie sprzętowym  Serwer musi posiadać wsparcie dla protokołu IPMI w wersji 2.0  Serwer musi posiadać nadmiarowe i hotswapowe wentylatory i zasilacze o mocy co najmniej 750W  Serwer musi posiadać kartę VGA  Serwer musi posiadać wysokość maksymalnie 2U do instalacji w standardowej szafie RACK 19 cali. Obudowa musi być dostarczona wraz z wszystkimi elementami mocującymi  Wraz z każdym z serwerów należy dostarczyć system operacyjny zgodny z dostarczonymi serwerami oraz oprogramowaniem do tworzenia kopii zapasowych |  |  |  |  |

Tabela 36 Serwery systemu tworzenia kopii zapasowych

#### Wymagania szczegółowe - klaster obliczeniowy HPC

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Klaster obliczeniowy HPC | Wymagania dotyczą:  HPCx.SRV.CG | System obliczeniowy do realizowania wielkoskalowych obliczeń naukowych  Liczba węzłów : minimum16 sztuk.  Klaster musi być podłączony poprzez sieć Fiber Channel do dedykowanej macierzy SAN wyposażonej w cache o pojemności minimum 16GB, wyposażonej w minimum 2 dyski 200GB SSD oraz 22 dyski 146GB 15K SAS z możliwością rozbudowy do minimum 240 dysków przy pojedyczej konfiguracji i co najmniej do minimum 480 dysków przy klastowaniu lub dodawaniu par kontrolerów.  Konfiguracja węzłów:  Procesory:   1. serwer musi posiadać zainstalowaną taką liczbę procesorów, aby osiągnąć łącznie minimum 20 rdzeni, 2. każdy rdzeń musi być taktowany zegarem minimum 2,4 GHz i realizować minimum 8 obliczeń zmiennoprzecinkowe w jednym cyklu zegarowym, 3. każdy procesor musi posiadać zintegrowany kontroler pamięci, 4. każdy serwer musi posiadać wydajność teoretyczną minimum 384GFlops   Pamięć operacyjna:   1. łączna zainstalowana pamięć musi wynosić minimum 128 GB, 2. moduły pamięci muszą być wyposażone w mechanizm korekcji błędnych bitów i być równomiernie zainstalowane przy każdym procesorze; 3. zastosowany musi być typ pamięci co najmniej PC3-14900   Dyski:   1. brak dysków twardych   Interfejsy sieciowe:   1. zainstalowane minimum dwa interfejsy sieciowe Gigabit Ethernet z funkcjonalnością uruchamiania serwera przez PXE; 2. zainstalowany minimum jeden interfejs 10 GbE lub InfiniBand HCA typu QDR 4X lub lepszy, zgodny z OpenFabrics OFED, 3. chipset karty IB HCA zgodny z chipsetem użytych przełączników IB,   Obudowa:   1. minimum 2 sloty na karty rozszerzeń 2. możliwość montażu w szafie rack 19 cali, 3. szyny teleskopowe do montażu w szafie rack, 4. wysokość maksimum 2U, 5. redundantne zasilacze o mocy wystarczającej do zasilenia wszystkich podzespołów w trybie zdegradowanym, wymienialne na gorąco (hot-swap), poziom redundancji N+1, 6. redundantne wentylatory wymienialne na gorąco (hot-swap), poziom redundancji N+1, 7. zainstalowany system operacyjny RedHat Enterprise Linux   Zarządzanie:   1. zgodne z IPMI 2.0 lub lepsze,   Wspierane systemy operacyjne:   1. co najmniej RedHat Enterprise Linux, Microsoft Windows Server, VMware vSphere |  |  |  |  |
| Sieć obliczeniowa | HPCx.SW.CG | Wszystkie węzły muszą być podłączone do przełączników 10GbE lub InfiniBand QDR, zgodnych z OpenFabrics OFED, o wystarczającej liczbie wolnych portów. Kable Ethernetowe lub InfiniBand QDR lub lepsze. W przypadku technologii IB Przełączniki muszą być wyposażone w procesory tego samego producenta co procesory w interfejsach InfiniBand zainstalowanych w węzłach. Przełączniki nie muszą być zarządzane.  Wszystkie węzły muszą być podłączone do dedykowanych dwóch przełączników SAN 8Gb FC posiadających aktywne 24 porty i obsadzone wkładkami 8Gb SFP SW. |  |  |  |  |
| System składowania danych obliczeniowych o dużej wydajności | Wymagania dotyczą:  HPC.STR.CG | Dedykowana przestrzeń dyskowa dla składowania danych tymczasowych dla obliczeń wielkoskalowych:   1. architektura klient – serwer, 2. komunikacja klient – serwer musi odbywać się przy pomocy protokołu o otwartym standardzie, 3. implementacja standardu musi być dostępna bez dodatkowych kosztów, 4. komunikacja klient – serwer musi odbywać się poprzez sieć użytą do zrealizowania komunikacji międzywęzłowej, 5. System musi zapewnić redundancję składowanych danych albo poprzez brak pojedynczego punktu awarii sprzętu (nie dotyczy przełączników), albo na poziomie danych, |  |  |  |  |

Tabela 37 Tabela bloku architektonicznego - klaster obliczeniowy HPC



#### Specyfikacja szczegółowa – system wirtualizacji serwerowej dla 8 serwerów 16 procesorów

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| System Wirtualizacji Serwerowej | Wymagania dotyczączą:  SCOx.SRV.CG,  SCOx.SRV.CZ | System Wirtualizacji Serwerowej musi zawierać nieograniczone licencje na ilość uruchomionych wirtualnych maszyn  SCO musi zawierać nieograniczone licencje na wielkość pamięci ram i ilość procesorów  SCO nie może wymagać zakupu dodatkowych licencji nie związanych z działaniem systemu wirtualizacji serwerowej.  Fizyczny serwer SCO musi wspierać 320 logicznych procesorów oraz 4TB pamięci RAM.  SCO musi umożliwiać tworzenie wirtualnych maszyn z 64 vCPU oraz 1TB vRAM oraz wirtualnymi dyskami o pojemności 64TB.  SCO musi przypisywanie VLAN dla poszczególnych maszyn wirtualnych  SCO musi zezwalać na współdzielenie maszyn wirtualnych pomiędzy użytkownikami.  SCO musi zapewniać równoważenie obciążenia ruchu sieciowego dla wirtualnych maszyn  SCO musi możliwość połączenia do konsoli wirtualnej maszyny.  SCO musi pozwalać na dodawanie własnych obrazów napędów CD/DVD.  SCO musi zapewniać możliwość alokowania zasobów dyskowych wirtualnych maszyn za pomocą sieci SAN oraz protokołu FC  SCO musi zapewniać możliwość migracji online maszyn wirtualnych przy zachowaniu wszystkich połączeń sieciowych i dyskowych.  SCO musi zapewniać dostęp do środowiska za pomocą interfejsu GUI.  SCO musi zapewniać dostęp do środowiska za pomocą API oraz CLI  SCO musi udostępniać mechanizmy pozwalające na automatyczne uruchomienie wirtualnej maszyny na innej maszynie fizycznej w przypadku awarii maszyny podstawowej.  Wszystkie maszyny fizyczne muszą pracować w trybie aktywnym w klastrze wysokiej dostępności.  SCO musi zapewniać możliwość zarządzania wieloma klastrami wysokiej dostępności.  SCO musi zapewniać możliwość wykonywania replikacji asynchronicznej VM na poziomie hypervisora.  SCO nie może zawierać pojedynczych punktów awarii. W przypadku pojedynczej awarii dowolnego komponentu musi dalej pracować wykorzystując komponenty nadmiarowe  SCO musi wspierać następujące systemy operacyjne Windows Server 2003/2008/2012, Windows XP/7/8, CentOS, Ubuntu, Red Hat Enterprise Linux, SUSE Linux Enterprise Server  Dla SCO należy dostarczyć dodatkowo 6 licencji Microsoft Windows Server 2012 DataCenter na 2CPU oraz 4 licencje Microsoft Windows Server 2012 Standard na 2CPU. |  |  |  |  |

Tabela 38 System Wirtualizacji Serwerowej



#### Wymagania szczegółowe - Monitoring aplikacji i usług

| **Komponent** | **Skrót / symbol** | **Wymagania szczegółowe** | **Proponowane rozwiązanie (sprzęt, marka, model itp. informacje)** | **Proponowana liczba sztuk** | **Spełnienie wymagań: TAK** | **Spełnienie wymagań: NIE** |
| --- | --- | --- | --- | --- | --- | --- |
| Monitoring aplikacji i usług | Wymagania dotyczą: MON.SRV.CG, MON.SRV.CZ | Oprogramowanie musi zapewniać monitorowanie agentowe oraz bezagentowe infrastruktury IT.  Licencja na monitorowany system musi dawać możliwość wyboru metody monitoringu agentowego bądź bezagentowego zarówno w momencie instalacji jak i w dowolnym momencie eksploatacji systemu monitoringu.  Zmiana metody monitoringu nie może pociągać za sobą konieczności zmiany, migracji bądź dokupowania dodatkowych licencji.  W ramach jednej licencji na monitorowany system musi być możliwość korzystania jednocześnie z monitorowania agentowego i bezagentowego.  Koszt agenta nie może być uzależniony od ewentualnej rozbudowy sprzętowej serwera na, którym jest on zainstalowany (instalacja dodatkowych procesorów).  Oprogramowanie musi zapewnić mechanizmy wzbogacania zdarzeń o dane umieszczone w zewnętrznych źródłach danych.  Oprogramowanie musi zapewniać możliwość rozszerzania wzorców monitorowania z wykorzystaniem WMI, SNMP, SSH.  Oprogramowanie musi zapewniać możliwość wykorzystania danych ze specjalizowanych systemów monitorowania poprzez mechanizmy integracji takie jak: pliki logów, trapy SNMP, odczyt informacji o zdarzeniach z bazy danych.  Oprogramowanie musi umożliwić wykonanie polecenia systemowego w oparciu o akcje automatyczne.  System musi być zbudowany z centralnego serwera zarządzającego oraz musi posiadać budowę modułową, umożliwiającą dostosowanie się do zmian monitorowanej infrastruktury.  Oprogramowanie musi wspierać możliwość rozbudowy do systemu klastrowego lub rozproszonego (wiele stacji monitorujących).  Oprogramowanie musi umożliwiać integrację z systemem Service Desk  Zarządzanie konfiguracją z poziomu interfejsu webowego oraz linii komend.  System musi monitorować fizyczne parametry infrastruktury IT takie jak zasilacze, wentylatory, punkty dystrybucji zasilania, czujniki, etc.  System musi monitorować systemy Linux/Unix oraz Windows i Mac OS, bazy danych, urządzenia sieciowe takie jak routery, przełączniki, zapory ogniowe, IDS/IPS.  System musi monitorować zmiany sieci komputerowych w warstwie drugiej oraz trzeciej, obciążenie urządzeń sieciowy w/w, przepustowości segmentów sieciowych.  System musi monitorować urządzenia umieszczone za translacjami NAT.  System musi monitorować poprawność wykonywania aplikacji webowych oraz serwerowych.  System musi integrować się z zewnętrznymi skryptami.  System musi mieć możliwość grupowania monitoringu we wspólne serwisy, grupowania urządzeń, grupowania procesów biznesowych.  System musi mieć dostęp do danych wydajnościowych systemów monitorowanych z poziomu bazy danych oraz interfejsu graficzne, w postaci tabeli oraz grafów.  System musi posiadać możliwość podejmowania problemów, umożliwiać komunikację między operatorami oraz dokumentowanie działań związanych z wydarzeniem awarii.  System musi posiadać własne statystyki na temat wydajności i opóźnień odpytywania serwisów.  System musi posiadać funkcjonalność generowania raportów dla tendencji, dostępności, wystąpienia problemów w formatach HTML, CSV, JSON, XML w postaci grafów oraz tabeli dla okresów godzinnych, dniowych, tygodniowych, miesięcznych oraz rocznych.  Oprogramowanie musi zapewniać dostęp do zdarzeń historycznych oraz powiadomień przez graficzny interfejs.  System musi posiadać przyjazny interfejs do przeszukiwania logów na podstawie interesujących fraz.  System musi posiadać możliwość graficznego przedstawiania wystąpienia danego logu, zliczać informację, trend oraz przedstawić odchylenie od poprawnego/normalnego wyniku.  Oprogramowanie musi umożliwiać kreowanie w nim użytkowników i grup z możliwością nadawania uprawnień.  System musi posiadać wersję mobilną wykorzystywane przez smart fony.  System musi posiadać moduł wykonawczy potrafiący wykonać określone czynności zdefiniowane przez administratora w przypadku wystąpienia problemu.  System musi integrować się z protokołem SMTP w celu wysyłania powiadomień mailowych.  System musi integrować się z bramką GSM w celu wysyłania powiadomień SMSowych.  Oprogramowanie musi wspierać, co najmniej 200 urządzeń w ramach standardowo dostarczonego systemu. |  |  |  |  |

Tabela 39 Monitoring aplikacji i usług