Usługa obsługi serwisowej i wsparcia technicznego dla wszystkich dostępnych funkcji na okres 12 miesięcy dla posiadanych przez Zamawiającego urządzeń Next Generation Firewall (dalej NGF)

Zamawiający posiada urządzenia:

Lp.	Opis urządzenia NGF	Typ pracy	Numer seryjny
1	Palo Alto PA-3410	Klaster HA	024101002951
2	Palo Alto PA-3410		024101001780
3	Panorama	Hyper-V	000702710981

z subskrypcjami dla pozycji 1 -2 do dnia 12.09.2024 r.:

- PAN-PA-3410-ATP-HA2 (Advanced Threat Prevention subscription for device in an HA pair),
- PAN-PA-3410-ADVURL-HA2 (Advanced URL Filtering subscription),
- PAN-PA-3410-DNS-HA2 (DNS security subscription)
- PAN-SVC-BKLN-3410 (Partner enabled premium suport)

z subskrypcjami dla pozycji 3 do dnia 24.08.2024 r.:

- PAN-SVC-BKLN-PRA-25 (Partner enabled premium support)

Wszystkie nazwy własne produktów i licencji użytych w niniejszym dokumencie dotyczą infrastruktury będącej w posiadaniu Zamawiającego. Dostawa urządzeń oraz oprogramowania wskazanych w formie nazw handlowych nie jest przedmiotem niniejszego postępowania.

1. W ramach wsparcia Wykonawca przedłuży posiadane przez Zamawiającego subskrypcje dla 2 urządzeń Palo Alto Pa-3410 oraz dla Panoramy, w okresie od dnia zawarcia umowy na okres 12 miesięcy:
   a) PAN-PA-3410-ATP-HA2 (Advanced Threat Prevention subscription for device in an HA pair),
   b) PAN-PA-3410-ADVURL-HA2 (Advanced URL Filtering subscription),
   c) PAN-PA-3410-DNS-HA2 (DNS security subscription)
   d) PAN-SVC-BKLN-3410 (Partner enabled premium suport)
   e) PAN-SVC-BKLN-PRA-25 (Partner enabled premium support)

2. W ramach wsparcia, o którym mowa w pkt 1, Zamawiający otrzyma możliwość korzystania z następujących usług świadczonych przez producenta:
   a) aktualizacji oprogramowania firmware do najnowszych wersji publikowanych przez producenta,
   b) aktualizacji bazy definicji IPS (Intrusion Prevention System),
   c) aktualizacji sygnatur aplikacji,
   d) dostępu do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych,
   e) pomocy technicznej.

3. W ramach obsługi serwisowej, Wykonawca udzieli gwarancji na urządzenia NGF Zamawiającego.

4. Gwarancja producenta będzie spełniać następujące warunki:
   a) wszelkie koszty usunięcia awarii (usług, części, sprzętu zastępczego i transportu) ponosi producent sprzętu lub autoryzowana przez niego firma serwisująca, przy czym poprzez awarię Zamawiający rozumie problem w prawidłowym funkcjonowaniu całej infrastruktury sieciowej bądź pojedynczego urządzenia całkowicie uniemożliwiający pracę systemu lub pojedynczego urządzenia. Awaria zgłaszana będzie drogą telefoniczną, a następnie potwierdzona za pomocą poczty elektronicznej,
   b) czas reakcji serwisu: najpóźniej do końca następnego dnia roboczego (tj. dnia, który nie jest dniem ustawowo wolnym od pracy w rozumieniu ustawy z dnia 18 stycznia 1951 r. o dniach wolnych od pracy, Dz. U. z 2020 r. poz. 1920, oraz sobót) od chwili dokonania zgłoszenia,
   c) przyjmowanie zgłoszeń w godzinach 8.00-16.00 w dni robocze drogą telefoniczną bądź za pomocą poczty elektronicznej,
   d) czas usunięcia awarii, tj. przywrócenia pełnej funkcjonalności całej infrastruktury sieciowej bądź pojedynczego urządzenia, w terminie maksymalnie do 3 dni roboczych od chwili dokonania zgłoszenia przez Zamawiającego (ostateczny termin wynikać będzie z oferty Wykonawcy),
   e) w przypadku awarii jednego z urządzeń trwającej dłużej niż 3 dni roboczych lub w przypadku wystąpienia jednoczesnej awarii obydwu urządzeń działających w klastrze Wykonawca zobowiązany jest niezwłocznie (tego samego dnia w przypadku awarii zgłoszonych do godziny 13.00, a w przypadku awarii zgłoszonych po godz. 13.00 następnego dnia) udostępnić podłączyć i skonfigurować na ten okres sprzęt o wydajności i funkcjonalności nie gorszej niż sprzęt uszkodzony, a w przypadku klastra urządzeń o parametrach – pozwalających na przywrócenie pełnej funkcjonalności klastra,
   f) wszelkie koszty usunięcia awarii (usług, części, sprzętu zastępczego i transportu) ponosi producent sprzętu lub autoryzowana przez niego firma serwisująca, przy czym poprzez awarię Zamawiający rozumie problem w prawidłowym funkcjonowaniu całej infrastruktury sieciowej bądź pojedynczego urządzenia całkowicie uniemożliwiający pracę systemu lub pojedynczego urządzenia.

5. W przypadku, gdy Wykonawca oferuje subskrypcje i wsparcie nie w pełni kompatybilne z urządzeniami NGF (pozycja 1 do 3 w tabeli powyżej) posiadanymi przez Zamawiającego, Zamawiający dopuszcza zaoferowanie w ramach wynagrodzenia subskrypcji i wsparcia wraz z urządzeniami NGF posiadającymi nie gorszą funkcjonalność niż urządzenia NGF posiadane przez Zamawiającego:

   System zabezpieczeń NGF jest to dedykowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej systemu występuje separacja modułu zarządzania (control-plane) i modułu przetwarzania danych (data-plane). Całość sprzętu i oprogramowania jest wspierana przez jednego producenta.

   Wymagania szczegółowe dotyczące systemu zabezpieczeń NGF:
   - brak ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej
   - musi być wyposażone w:
     - minimum 12 interfejsów 1/10GE miedzianych (RJ45)
     - minimum 10 interfejsów 1/10GE SFP+. Należy dostarczyć minimum 8 wkładek 10GE SR.
     - minimum 4 interfejsy 25GE – wkładki SFP28. Należy dostarczyć minimum 2 wkładki 25GE SR.
   - musi spełniać co najmniej następujące parametry wydajnościowe:
     - Minimum 11.5 Gbps (ruch typu „appmix") dla Firewall/kontroli aplikacji
     - Minimum 5,7 Gbps (ruch typu „appmix") dla Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware
     - Minimum 144000 nowych połączeń (sesji) na sekundę
     - Minimum 1400000 równoległych/jednoczesnych zestawionych sesji
   - Jako scenariusz Firewall/kontroli aplikacji Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych. Jako scenariusz

Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych, inspekcje IPS, Antywirus, Anty Spyware. Zakres kontroli musi też obejmować przesyłanie plików do sandboxa lokalnego i chmurowego w tym przechwytywanie i blokowanie plików określonego typu. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla urządzenia sygnaturami IPS, antywirus i antyspyware.

- musi spełniać co najmniej następujące parametry wydajnościowe dla ruchu szyfrowanego (IPSEC VPN, SSL VPN):
  - Minimum 6.5 Gbps dla IPSEC VPN
  - Minimum 3000 tuneli IPSEC VPN (site-to-site)
  - Minimum 1000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN.

  Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji, lub jeżeli dedykowany klient VPN (co najmniej dla Windows) oferowany przez producenta firewall wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla maksymalnej jego wydajności tzn. dla 1000 jednoczesnych użytkowników.
- musi posiadać dysk Flash SSD o pojemności minimum 450GB.
- musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN.
- musi umożliwiać działanie w co najmniej trzech trybach pracy:
  - rutera (tzn. w warstwie 3 modelu OSI),
  - przełącznika (tzn. w warstwie 2 modelu OSI),
  - w trybie pasywnego nasłuchu (sniffer).
- Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.)
- musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3.
- musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
- musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej:
  - oznaczania pakietów znacznikami DiffServ,
  - ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego,
  - utworzenia co najmniej 8 klas ruchu sieciowego,
  - przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
- musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
- musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.
- musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu.
- musi obsługiwać wirtualne instancje firewalli/systemów/domen/kontekstów i posiadać możliwość rozbudowy do 10 takich systemów za pomocą licencji. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych:
  - Tablic routingu
  - Polityk bezpieczeństwa obejmujących: System IPS, System ochrony antymalware/antyspyware, System ochrony antywirus
  - Koncentratorów VPN dla zdalnego dostępu
- musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu.

- musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active.
- musi wspierać obsługę klastrowania dla kilku Data Center, gdzie urządzenia firewall umieszczone są w różnych Data Center (np. trzy ośrodki Data Center, gdzie w każdym mamy po dwa urządzenia). W ramach tej funkcji urządzenie musi się potrafić tworzyć klaster z minimum 6 urządzeń.
- musi posiadać wspierać funkcjonalność Network Packet Broker, gdzie dany ruch może być wysłany dodatkowo do kolejnych urządzeń/narzędzi bezpieczeństwa takich jak systemy SIEM, IPS/IDS, nagrywarki ruchu.
- polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 10000 reguł polityki bezpieczeństwa oraz obsługę minimum 200 stref bezpieczeństwa.
- musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65535 dostępnych portach.
- musi wykrywać co najmniej 3000 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.
- musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM), w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce.
- musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
- musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
- musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
- musi zapewniać ochronę przed atakami typu „Drive-by-download".
- musi posiadać możliwość zdefiniowania ruchu SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
- musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
- musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o:
  - Microsoft Active Directory,
  - usługi katalogowe LDAP,
  - serwery Terminal Services,
  - logi z syslog,
- polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
- musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur IPS/IDS musi

być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi. Zamawiający wymaga dostarczenia licencji na IPS w chwili zakupu urządzenia.

- musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb. Baza sygnatur AV musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Moduł AV musi być uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduł inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Zamawiający wymaga dostarczenia licencji na ochronę antywirusową w chwili zakupu urządzenia.
- musi zapewniać ochronę przed atakami typu Spyware. Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi być uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta była uruchamiana per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. Zamawiający wymaga dostarczenia licencji na silnik Antyspyware w chwili zakupu urządzenia.
- musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole). Zamawiający wymaga dostarczenia licencji na ochronę DNS w chwili zakupu urządzenia.
- Funkcja ochrony DNS musi wykrywać ataki bazującym na tunelowaniu ruchu poprzez protokół DNS.
- Urządzenie musi za pomocą sprawdzania DNS (np. w połączeniu z URL Filtering) wykonywać klasyfikację ryzyka otwieranych stron Web – wykrywać nowo zarejestrowane domeny, mieć widzę na temat domen związanych ze złośliwym działaniem, analizować zawartość stron phishing'owych.
- musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
- musi posiadać funkcjonalność URL Flitering. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. Zamawiający wymaga dostarczenia licencji na URL Filtering w chwili zakupu urządzenia.
- musi posiadać funkcjonalność ochrony przed atakami zero-day i współpracy z sandboxem. Urządzenie musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand Box" plików różnych typów co najmniej exe i dll, przechodzących przez firewall z wydajnością

modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day. Zamawiający nie wymaga dostarczenia licencji w chwili zakupu urządzenia.

- urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).
- system zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach w szczególności Urządzenie musi mieć zdefiniowane w systemie co najmniej dwa konta typu:
- administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu.
- operator, który ma możliwość tylko odczytu konfiguracji.
- musi umożliwiać uwierzytelnianie administratorów za pomocą:
  - bazy lokalnej,
  - serwera LDAP,
  - RADIUS lub TACACS+
  - SAML 2,0
- musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
- praca na urządzeniu musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. commit). Przed zatwierdzaniem zmian na urządzeniu musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej. Funkcja musi być dostępna co najmniej w interfejsie GUI.
- musi zapewniać interfejs API (JSON, REST, XML lub inny) będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
- musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. Urządzenie musi mieć możliwość przywrócenia konfiguracji z określnego dnia, w którym były dokonywane zmiany, tzn. po każdym zapisie konfiguracji na urządzeniu powinna być automatycznie zapisywana kompletna konfiguracja, a podczas wyboru konfiguracji musi być widoczna data zapisania konfiguracji.
- musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall/kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest, aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. w innych systemach wirtualnych.
- musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG.
- musi być wyposażone w redundantne zasilacze typu AC pracujące redundantnie.