Załącznik nr 9 do SWZ

Opis przedmiotu zamówienia
Modernizacja urządzeń sieci szkieletowej w budynkach
Akademii Muzycznej im. Karola Lipińskiego we Wrocławiu

I. Dostawa urządzeń.

1. Minimalne wymagania dla firewalla w trybie „klastrze" HA – 1 sztuka
   W tabeli umieszczono minimalne wymagania dla firewalla. Zamawiający wymaga, aby urządzenie nie tylko spełniało warunki zawarte w tabeli, ale było również wyposażone we wszystkie elementy w niej przedstawione.

L.p.	Właściwość	Opis
1.	Architektura urządzenia	- Urządzenie musi stanowić dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań serwerowych bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia - Urządzenie musi pełnić rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall) - Urządzenie musi być wyposażone w co najmniej 12 interfejsów 10/100/1000 Mbps Ethernet (RJ45),oraz 4 Gigabit Ethernet SFP - Zamawiający akceptuje wkładki o parametrach równoważnych lub lepszych, bez utraty funkcjonalności i wydajności, kompatybilnych z dostarczonym sprzętem (równoważne tj. spełniające wszystkie minimalne wymagania specyfikacji technicznej). - Urządzenie musi obsługiwać interfejsy VLAN (802.1Q) na interfejsach fizycznych – min. 1k sieci VLAN - Urządzenie musi być wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band - Urządzenie musi być wyposażone w port USB 2.0 lub nowszy - Urządzenie musi posiadać zasilacze redundantne umożliwiające zasilanie prądem przemiennym 230V - Urządzenie o wysokości maksymalnej 1RU, przystosowane do montażu w szafie rack 19'' (wymagane jest dostarczenie niezbędnych elementów montażowych)
2.	Parametry wydajnościowe	- Urządzenie musi posiadać przepustowość dla uruchomionych modułów firewall'a, kontroli aplikacji i systemu IPS na poziomie co najmniej 2Gb/s dla pakietów o wielkości maksymalnie 1024 bajtów - Maksimum 1500 tuneli IPSEC VPN (site-to-site) z sumaryczną przepustowością co najmniej 950Mbps dla pakietów o wielkości maksymalnie 1024 bajtów - Maksymalna liczba sesji (z kontrolą aplikacji) na poziomie 1mln z możliwością zestawiania co najmniej 14k nowych połączeń na sekundę
3.	Funkcjonalność urządzenia	- Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej - Urządzenie musi umożliwiać podział na niezależne logiczne instancje. Urządzenie musi posiadać możliwość uruchomienia minimum 5 w pełni funkcjonalnych logicznych instancji tzw. wirtualnych firewalli, tj. wirtualnych instancji w ramach jednego urządzenia fizycznego, pozwalających na niezależną konfigurację i separację. - Urządzenie musi posiadać możliwość uruchomienia urządzenia w trybie firewall'a L3 oraz w trybie transparentnym

		- Urządzenie musi obsługiwać routing statyczny i dynamiczny (co najmniej: RIP, OSPF, BGP) - Urządzenie musi posiadać możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory - Urządzenie musi obsługiwać funkcjonalność Network Address Translation (NAT) wraz z Port Address Translation (PAT) - Urządzenie musi zapewniać mechanizmy redundancji, w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby - Urządzenie musi zapewniać funkcjonalność tzw. Firewall'a Next-Generation w zakresie: − systemu automatycznego wykrywania i klasyfikacji aplikacji − systemu IPS − systemu antymalware - Urządzenie musi zapewniać możliwość dodatkowej rozbudowy funkcjonalności w zakresie systemu filtracji ruchu w oparciu o URL. - Urządzenie musi posiadać funkcjonalność wykrywania aplikacji, zapewniającą: − możliwość klasyfikacji ruchu i wykrywania co najmniej 3,5k aplikacji. − możliwość definiowania sygnatur aplikacyjnych pozwalających na skonfigurowanie opisu dowolnej aplikacji i wykorzystania go do automatycznego wykrywania oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz raportach. - Urządzenie musi posiadać funkcjonalność systemu IPS zapewniającego: − możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system) − możliwość wykrywania i blokowania szerokiej gamy zagrożeń, w tym: ▪ złośliwe oprogramowanie ▪ skanowanie sieci ▪ ataki na usługę VoIP ▪ próby przepełnienia bufora ▪ ataki na aplikacje P2P ▪ zagrożenia dnia zerowego − możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna) − możliwość inspekcji warstwy sieciowej i informacji zawartych w nagłówkach pakietów oraz również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego, włącznie z możliwością sprawdzania zawartości pakietu − możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń − wiele możliwości reakcji na zdarzenia w tym takie, jak: ▪ tylko monitorowanie ▪ blokowanie ruchu zawierającego zagrożenia ▪ zapisywanie pakietów − możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji

		− możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie - możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego - Urządzenie musi posiadać funkcjonalność polegająca na wykrywaniu i śledzeniu transferu następujących kategorii plików w ruchu sieciowym: − pliki graficzne − pliki PDF − pliki wykonywalne − pliki multimedialne − pliki pakietu Office − pliki skompresowane - Urządzenie musi posiadać możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: − HTTP − SMTP − FTP − IMAP − POP3 - Urządzenie musi posiadać wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i umożliwiać: − sprawdzenie reputacji plików w systemie globalnym − sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze) − statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu - możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o: - systemach operacyjnych - serwisach - otwartych portach, aplikacjach - zagrożeniach
4.	Zarzadzanie	- Zarządzanie musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli - dedykowana platforma zarządzająca w formie maszyny wirtualnej umożliwiająca co najmniej: - agregację wszystkich zdarzeń i dynamiczne dostrajanie systemu IDS/IPS oraz centralne monitorowanie i analizę, - konfigurowanie limitu powtórzeń danego zdarzenia - zarządzanie oparte o role z zapewnieniem różnych widoków interfejsu - automatyczną konfigurację pobierania zestawów sygnatur na najnowsze zagrożenia - zapewnia informowanie o zagrożeniach poprzez ▪ wysłanie e-maila, ▪ wysłanie trap SNMP, ▪ przesłanie informacji do serwera Syslog, ▪ uruchomienie skryptu użytkownika

		▪ wysłanie informacji do jednego lub kilku rozwiązań typu SIEM poprzez zaszyfrowane łącze - w ramach funkcji kategoryzacji zapytań HTTP (URL filtering) rozwiązanie ma mieć możliwość interaktywnego blokowania z resetowaniem zapytań. W ramach tej funkcji jest zapewniona możliwość zdefiniowania własnej strony internetowej ostrzegającej o naruszeniu polityki kontroli dostępu i zrzuceniu zablokowanej próby połączenia
5.	Dodatkowe wymagania	- Urządzenie musi być wyposażone w zasilacz typu AC, o mocy maksymalnej 250W. - Wraz z każdym urządzeniem muszą być dostarczone następujące kable i wkładki: − Wkładka optyczna MultiMode Ethernet 1Gb/s SFP – sztuk 4 − Zestaw okablowania pozwalający zestawić klaster HA w trybie active/active z maksymalną oferowaną przez urządzenie prędkością długość min. 3 metry – jeden zestaw okablowania na parę urządzeń. - Przewód zasilający 230V AC - sztuk 2 - Urządzenie musi być wyposażone w elektroniczny nośnik danych lub dysk SSD wielkości minimum 100 GB. Dyski obrotowe nie są akceptowalne.
6.	Gwarancja i serwis	Zamawiający wymaga zapewnienia serwisu gwarancyjnego opartego o usługi producenta dostarczanego sprzętu dla sprzętu i oprogramowania na okres co najmniej 36 miesięcy. Wymagany reżim serwisu to (8x5xNBD) wymiana uszkodzonego urządzenia (w lokalizacji Zamawiającego) na następny dzień roboczy. Zamawiający wymaga również zapewnienia prawa do bezpośredniego dostępu do pomocy technicznej producenta, jego bazy wiedzy w celu wsparcia przy rozwiązywaniu problemów eksploatacyjnych oraz aktualizacji oprogramowania. Zgłoszenie awarii (potrzebę wsparcia technicznego) Zamawiający dokona według własnego wyboru: w systemie Producenta lub za pośrednictwem Wykonawcy.
7.	Licencje	- Licencje związane z dostarczonym sprzętem muszą być zarejestrowane na użytkownika końcowego tj. Zamawiającego. - Jeżeli którakolwiek z funkcjonalności opisanych wyżej wymaga dodatkowych licencji, należy je dostarczyć. - subskrypcja IPS i filtracji URL na okres minimum 36 miesięcy

2. Minimalne wymagania dla przełącznika dostępowego – 6 sztuk
   W tabeli umieszczono minimalne wymagania dla jednego przełącznika. Zamawiający wymaga, aby urządzenie nie tylko spełniało warunki zawarte w tabeli, ale było również wyposażone we wszystkie elementy w niej przedstawione.

L.p.	**Właściwość**	**Opis**
1.	Zasilanie i chłodzenie	- Redundantne zasilanie i chłodzenie, pozwalające na wymianę uszkodzonego elementu w tzw. trybie „na gorąco” (bez przerwy w pracy urządzenia) - Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia - Redundantne wentylatory
2.	Fizyczne porty połączeniowe	- 48 portów – o przepustowości 1 Gigabit Ethernet POE+ - 4 portów – o przepustowości 10 Gigabit Ethernet SFP+
3.	Wkładki światłowodowe zapewniające	- 48 wkładek 1 Gigabit Ethernet POE+ - 4 wkładek 10 Gigabit Ethernet SFP+ 9 (zasięg działania do 300 m na OM3 lub 400 m na OM4)

	prawidłowe działanie urządzenia	- Zamawiający akceptuje wkładki o parametrach równoważnych lub lepszych, bez utraty funkcjonalności i wydajności, kompatybilnych z dostarczonym sprzętem (równoważne tj. spełniające wszystkie minimalne wymagania specyfikacji technicznej).
4.	Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:	- Przepustowość w ramach stosu - 80Gb/s - 8 urządzeń w stosie - Zarządzanie poprzez jeden adres IP - Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad
5.	Parametry wydajnościowe:	- Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate) - Bufor pakietów – min. 6MB - Obsługa: • min. 1024 sieci VLAN • min. 16.000 adresów MAC • min. 3.000 tras IPv4 • min. 1.500 tras IPv6 - Pamięć: • DRAM – min. 2GB • Pamięć flash – min. 4GB
6.	Wymagane wsparcie dla mechanizmów związanych z zapewnieniem ciągłości pracy sieci:	- IEEE 802.1w Rapid Spanning Tree - Per-VLAN Rapid Spanning Tree (PVRST+) - IEEE 802.1s Multi-Instance Spanning Tree - Obsługa 64 instancji protokołu STP
7.	Wymagane mechanizmy związane z bezpieczeństwem sieci:	- Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level) - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL - Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC - Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X - Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem - Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176 - 1500 wpisów dla list kontroli dostępu (Security ACE) - Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres /uwierzytelnianie w oparciu o portal www) - Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard - Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych

		komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard) - Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+ - Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia) - Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch oraz switch-host) - Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing) - Funkcja Private VLAN
8.	Wymagane mechanizmy związane z zapewnieniem jakości usług w sieci:	- Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi - Implementacja algorytmu Shaped Round Robin dla obsługi kolejek - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority) - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP - Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi (policing, rate limiting) - Kontrola sztormów dla ruchu broadcast/multicast/unicast - Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
9.	Wymagana obsługa protokołów routingu:	- Routing statyczny dla IPv4 i IPv6 - Routing dynamiczny – RIP, OSPF (do 1000 tras) - Policy-based routing (PBR) - Obsługa protokołu redundancji bramy (VRRP)
10.	Wymagane mechanizmy zarządzania urządzeniem:	- Port konsoli - Dedykowany port Ethernet do zarządzania out-of-band - Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją - Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 - Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów - Port USB umożliwiający podłączenie zewnętrznego nośnika danych z możliwością uruchomienia z nośnika danych umieszczonego w porcie USB
11.	Inne	- Wymagana obsługa protokołu NTP - Obsługa IGMPv1/2/3 i MLDv1/2 Snooping - Obsługa protokołu LLDP i LLDP-MED. - Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC - Wymagana obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego - Wymagana obsługa mechanizmów SPAN i RSPAN do lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegającą na kopiowaniu

		pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego. - Wymagana możliwość uruchomienia funkcji serwera DHCP - Wymagane predefiniowane (prekonfigurowane) wzorce konfiguracji portów z ustawieniami rekomendowanymi zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.) - Wymagana możliwość uruchamiania skryptów Python w zależności od zdarzeń, jakie zaszły w urządzeniu - Możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU - Wsparcie dla próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym – NetFlow - Możliwość enkapsulacji ruchu w pakiety VXLAN - próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym - NetFlow – obsługa min 16.000 strumieni - Wbudowany analizator pakietów - Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie
12.	Gwarancja i serwis	Zamawiający wymaga zapewnienia serwisu gwarancyjnego opartego o usługi producenta dostarczanego sprzętu dla sprzętu i oprogramowania na okres co najmniej 36 miesięcy. Wymagany reżim serwisu to (8x5xNBD) wymiana uszkodzonego urządzenia (w lokalizacji Zamawiającego) na następny dzień roboczy. Zamawiający wymaga również zapewnienia prawa do bezpośredniego dostępu do pomocy technicznej producenta, jego bazy wiedzy w celu wsparcia przy rozwiązywaniu problemów eksploatacyjnych oraz aktualizacji oprogramowania. Zgłoszenie awarii (potrzebę wsparcia technicznego) Zamawiający dokona według własnego wyboru: w systemie Producenta lub za pośrednictwem Wykonawcy.
13.	Licencje	- Licencje związane z dostarczonym sprzętem muszą być zarejestrowane na użytkownika końcowego tj. Zamawiającego. - Jeżeli którakolwiek z funkcjonalności opisanych wyżej wymaga dodatkowych licencji, należy je dostarczyć.

3. Minimalne wymagania dla przełącznika głównego – 2 sztuk

W tabeli umieszczono minimalne wymagania dla jednego przełącznika. Zamawiający wymaga, aby urządzenie nie tylko spełniało warunki zawarte w tabeli, ale było również wyposażone we wszystkie elementy w niej przedstawione.

L.p.	**Właściwość**	**Opis**
1.	Obudowa	- nie mniejsza niż 6U z możliwością zainstalowania co najmniej 2 dedykowanych kart liniowych
1.	Zasilanie i chłodzenie	- Redundantne zasilanie i chłodzenie, pozwalające na wymianę uszkodzonego elementu w tzw. trybie „na gorąco" (bez przerwy w pracy urządzenia) - Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia - Redundantne wentylatory
2.	Fizyczne porty połączeniowe	- 48 portów – o przepustowości 1 Gigabit Ethernet UPOE+ - 24 porty – o przepustowości 10 Gigabit Ethernet SFP+
3.	Wkładki światłowodowe zapewniające	- 48 wkładek 1 Gigabit Ethernet POE+ - 24 wkładki 10 Gigabit Ethernet SFP+ 9 (zasięg działania do 300 m na OM3 lub 400 m na OM4)

	prawidłowe działanie urządzenia	- Zamawiający akceptuje wkładki o parametrach równoważnych lub lepszych, bez utraty funkcjonalności i wydajności, kompatybilnych z dostarczonym sprzętem (równoważne tj. spełniające wszystkie minimalne wymagania specyfikacji technicznej).
4.	Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:	- Przepustowość w ramach stosu - 80Gb/s - Zarządzanie poprzez jeden adres IP - Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad
5.	Parametry wydajnościowe:	- Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate) - Bufor pakietów – min. 6MB - Obsługa: • min. 1024 sieci VLAN • min. 16.000 adresów MAC • min. 3.000 tras IPv4 • min. 1.500 tras IPv6 - Pamięć: • DRAM – min. 2GB • Pamięć flash – min. 4GB • Dysk 240GB M2 SATA
6.	Wymagane wsparcie dla mechanizmów związanych z zapewnieniem ciągłości pracy sieci:	- IEEE 802.1w Rapid Spanning Tree - Per-VLAN Rapid Spanning Tree (PVRST+) - IEEE 802.1s Multi-Instance Spanning Tree - Obsługa 64 instancji protokołu STP
7.	Wymagane mechanizmy związane z bezpieczeństwem sieci:	- Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level) - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL - Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC - Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X - Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem - Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176 - 1500 wpisów dla list kontroli dostępu (Security ACE) - Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www) - Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard

		- Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard) - Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+ - Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia) - Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch oraz switch-host) - Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing) - Funkcja Private VLAN
8.	Wymagane mechanizmy związane z zapewnieniem jakości usług w sieci:	- Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi - Implementacja algorytmu Shaped Round Robin dla obsługi kolejek - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority) - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy /docelowy adres IP, źródłowy/docelowy port TCP - Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi (policing, rate limiting) - Kontrola sztormów dla ruchu broadcast/multicast/unicast - Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
9.	Wymagana obsługa protokołów routingu:	- Routing statyczny dla IPv4 i IPv6 - Routing dynamiczny – RIP, OSPF (do 1000 tras) - Policy-based routing (PBR) - Obsługa protokołu redundancji bramy (VRRP)
10.	Wymagane mechanizmy zarządzania urządzeniem:	- Port konsoli - Dedykowany port Ethernet do zarządzania out-of-band - Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją - Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 - Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów - Port USB umożliwiający podłączenie zewnętrznego nośnika danych z możliwością uruchomienia z nośnika danych umieszczonego w porcie USB
11.	Inne	- Wymagana obsługa protokołu NTP - Obsługa IGMPv1/2/3 i MLDv1/2 Snooping - Obsługa protokołu LLDP i LLDP-MED. - Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC - Wymagana obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

		- Wymagana obsługa mechanizmów SPAN i RSPAN do lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego. - Wymagana możliwość uruchomienia funkcji serwera DHCP - Wymagane predefiniowane (prekonfigurowane) wzorce konfiguracji portów z ustawieniami rekomendowanymi zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.) - Wymagana możliwość uruchamiania skryptów Python w zależności od zdarzeń, jakie zaszły w urządzeniu - Możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU - Wsparcie dla próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym – NetFlow - Możliwość enkapsulacji ruchu w pakiety VXLAN - próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym - NetFlow – obsługa min 16.000 strumieni - Wbudowany analizator pakietów - Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie
12.	Gwarancja i serwis	Zamawiający wymaga zapewnienia serwisu gwarancyjnego opartego o usługi producenta dostarczanego sprzętu dla sprzętu i oprogramowania na okres co najmniej 36 miesięcy. Wymagany reżim serwisu to (8x5xNBD) wymiana uszkodzonego urządzenia (w lokalizacji Zamawiającego) na następny dzień roboczy. Zamawiający wymaga również zapewnienia prawa do bezpośredniego dostępu do pomocy technicznej producenta, jego bazy wiedzy w celu wsparcia przy rozwiązywaniu problemów eksploatacyjnych oraz aktualizacji oprogramowania. Zgłoszenie awarii (potrzebę wsparcia technicznego) Zamawiający dokona według własnego wyboru: w systemie Producenta lub za pośrednictwem Wykonawcy.
13.	Licencje	- Licencje związane z dostarczonym sprzętem muszą być zarejestrowane na użytkownika końcowego tj. Zamawiającego. - Jeżeli którakolwiek z funkcjonalności opisanych wyżej wymaga dodatkowych licencji, należy je dostarczyć.

II. Usługa migracji z aktualnie posiadanego przez Zamawiającego środowiska informatycznego

Wykonawca zobowiązany jest dostarczony sprzęt zamontować, uruchomić i skonfigurować do współpracy z siecią Akademii Muzycznej. oraz z systemem transmisji głosu opartym na rozwiązaniu Cisco 2901/K9. W zakresie uruchomienia sprzętu wchodzi przeniesienie konfiguracji ze starego środowiska na nowe oraz zabezpieczenie urządzeń zgodnie z najlepszymi praktykami w zakresie bezpieczeństwa sieci.

Wykonawca zintegruje dostarczone produkty zarówno pomiędzy sobą, jak i z elementami systemu teleinformatycznego Zamawiającego w sposób wynikający z uzgodnień z Zamawiającym (określonych podczas ustaleń przedwdrożeniowych) oraz przewidzianych przez dokumentację produktów, zgodnie z najlepszymi praktykami i doświadczeniem Wykonawcy.

Wykonawca zobowiązany jest do przeniesienia obecnych polityk, reguł dostępu i całej konfiguracji z obecnego Firewalla, głównego przełącznika oraz przełączników dostępowych Zamawiającego do nowego systemu.

W ramach wdrożenia Wykonawca zgodnie z zaakceptowanym projektem technicznym:

1) Zainstaluje dostarczane urządzenia w szafach RACK, podłączy do sieci: elektrycznej i LAN, skonfiguruje zarządzanie urządzeniami.
2) Wykona organizacje okablowania elektrycznego i LAN wewnątrz sieci RACK
3) Dostosuje konfigurację istniejących urządzeń, aby umożliwić podłączenie dostarczonych urządzeń.
4) Wykona konfigurację urządzeń właściwą dla docelowego środowiska, obejmującą migrację konfiguracji z posiadanych przez Kupującego urządzeń sieciowych na dostarczane urządzenia.
5) Skonfiguruje mechanizmy ochrony typu IPS oraz antymalware.
6) Wykona przełączenie ruchu sieciowego na dostarczone urządzenia.
7) Wykona testy akceptacyjne (plan testów Sprzedawca przedstawi Kupującemu do akceptacji).
8) Wykonana dokumentację powykonawczą i procedury eksploatacyjne.

W ramach prac związanych z konfiguracją sprzętu Wykonawca zobowiązany jest przeszkolić personel Zamawiającego w zakresie zaimplementowanej w urządzeniu konfiguracji. Zamawiający przewiduje, że ww. prace nie przekroczą 7 dni roboczych inżyniera specjalisty. Prace realizowane będą w Akademii Muzycznej im. Karola Lipińskiego we Wrocławiu przy pl. Jana Pawła II nr 2 50-043 Wrocław.
Zamawiający jest w posiadaniu następującego sprzętu:

1. Główny przełącznik w stosie oparty o następujące modele

Producent	Model	Numer seryjny	Software
Cisco	WS-C3750G-12S-S (V14)	FCZ143271NX	12.2(55) SE7
Cisco	WS-C3750X-24T-S (V07)	FDO1913H10X	12.2(55) SE7
Cisco	WS-C3750X-48T-S (V02)	FDO1548P045	12.2(55) SE8

2. Firewall

Producent	Model	Numer seryjny	Software
Cisco	ASA5510	JMX1132L0GC	9.0(3)

3. VOIP

Producent	Model	Numer seryjny	Software
Cisco	2901/K9	FGL15472MP	15.0(1r)M12

4. Przełączniki dostępowe „PD” rozmieszczone na terenie Uczelni

Producent	Model	Numer seryjny	Software
Cisco	WS-C2960G-48TC-L (V03)	FOC1319Y2YG	12.2(50) SE
Cisco	WS-C2960G-24TC-L (V02)	FOC1024X19H	12.2(25) FX
Cisco	WS-C2960G-25TC-L (V03)	FOC1129Z43A	12.2(25) SSE4
Cisco	WS-C2960G-24TC-L (V03)	FOC1129Z44Q	12.2(25) SEE4
Cisco	WS-C2960G-25TC-L (V03)	FOC1129X2DB	12.2(25) SEE4
Cisco	WS-C2960-48TC-L (V05)	FOC1414U08E	12.2(44) SE6

Wykonawca zapewni miesięczną opiekę powdrożeniową w ramach której zapewni:
- stabilną pracę wdrożonego systemu
- dodawanie nowych, określonych przez Klienta funkcji
- dostosowanie systemu do nowych rozwiązań technologicznych
- porady eksperckie
- dodatkowe integracje z systemami wewnętrznymi Opieka będzie realizowana zdalnie lub lokalnie w zależności od metodyki właściwej dla zdefiniowanego problemu według decyzji Wykonawcy.