Miejscowość: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Data: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Załącznik nr 1**

**FORMULARZ OFERTOWY**

**Zapytanie ofertowe nr 4/ sieć komputerowa**

Nazwa Wykonawcy:

Adres:

NIP:

Nr telefonu:

Adres e-mail:

Dane osoby do kontaktu:

W odpowiedzi na zapytanie ofertowe pn. *Zapytanie ofertowe nr 4/ sieć komputerowa,* oferuję wykonanie przedmiotu zamówienia, zgodnie z wymogami i zakresem określonym w zapytaniu ofertowym, za:

|  |  |  |  |
| --- | --- | --- | --- |
| **Przedmiot zamówienia** | **Ogółem wartość netto w PLN** | **Wartość podatku VAT w PLN** | **Ogółem wartość brutto w PLN** |
| **Dostawa i konfiguracja urządzeń sieci komputerowej** |  |  |  |

Całkowita wartość zamówienia brutto słownie:

1. Ceny wskazane w tabeli uwzględniają wszystkie koszty związane z wykonaniem przedmiotu zamówienia i są cenami stałymi w okresie obowiązywania umowy.
2. Cały przedmiot zamówienia będzie posiadał aktualne atesty i certyfikaty bezpieczeństwa poświadczające zgodność z normami obowiązującymi w Unii Europejskiej oraz zgodności i certyfikaty określone w zapytaniu ofertowym.
3. Zobowiązujemy się do wykonania przedmiotu zamówienia zgodnego podanymi poniżej minimalnymi parametrami, opisami i funkcjami z zastosowaniem następujących urządzeń i materiałów:

(***W każdym wierszu tabeli należy podać informację czy/jak oferowany sprzęt spełnia wymagania Zamawiającego. Dopuszcza się wypełnienie wierszy w formule TAK/NIE. W przypadku braku zamieszczenia informacji (braku wypełnienia) w którymkolwiek z obowiązkowych pól, oferta zostanie odrzucona. Wykonawca tam gdzie jest to możliwe wskazuje również „Typ/model oferowanego urządzenia” oraz „Producenta”).***

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Minimalne wymagania i parametry techniczne przedmiotu zamówienia** | **Potwierdzenie spełnienia /**  **Parametry oferowane[[1]](#footnote-1)** | |
| **Urządzenia tworzące zamawianą sieć komputerową** | | | |
| **1.** | **Urządzenie typu Firewall - 2 szt.** | **Typ/model oferowanego urządzenia** |  |
| 1. Typ urządzenia:  * Urządzenie klasy UTM (Unified Threat Management) * Urządzenie typu wolnostojącego appliance  1. Wyposażenie:  * 4 interfejsy LAN typu 1000Base-T oraz dwa interfejsy 10 Gbps SFP+ * 2 interfejsy WAN 10Gbps SFP+ oraz dwa interfejsy WAN RJ45 2.5Gbps * Interfejs USB do podłączenia modemu 3G/4G/LTE * Dysk twardy o pojemności 1TB  1. Parametry wydajnościowe:  * Wydajność zapory ogniowej L3 z NAT 5 Gbps * Wydajność urządzenia z włączonymi wszystkimi funkcjami bezpieczeństwa (NAT, VPN (Split-tunnel), filtrowanie treści, traffic shaping, anti-virus/anti-phishing, IPS): 2 Gbps * Maksymalna ilość połączeń: 250000 * Przepustowość dla ruch VPN: 2Gbps * Maksymalna liczba sesji VPN: 1000  1. Parametry fizyczne  * wysokość 1RU * możliwość montażu w szafie 19” * praca w temperaturach 0 – 40 st.C * waga do 5kg * urządzenie wyposażone w dwa zasilacze 230V AC  1. Urządzenie realizuje funkcje zintegrowanego systemu zarządza­nia zagrożeniami obejmującego:  * Firewalling ruchu sieciowego w warstwie 3 - filtracja na podstawie: * protokołu sieciowego (TCP/UDP/dowolny); * źródłowe adresy IP * źródłowe porty * docelowe adresy IP * docelowe porty * Tworzenie niezależnego filtru blokującego ruch sieciowy w warstwie 3 dla ruchu kierowanego do łącza komórkowego 3G/4G/LTE * Możliwość zablokowania lub ograniczenia dla określonych adresów IP odpowiedzi na ICMP ping oraz odpowiedzi do wbudowanego serwera WEB dla interfejsów zewnętrznych * Firewalling ruchu aplikacyjnego wg. typu aplikacji w warstwie 7: * Blogging * Email * File Sharing * Gaming * News * Online backup * Peer-to-peer * Social web * Software updates * Anti-virus updates * Sports * Video * Music * VOIP * Video Conferencing * Web file sharing * Możliwość blokowania ruchu do zdefiniowanego serwera http przez podanie domeny sieciowej * Możliwość blokowania ruchu internetowego pochodzącego lub wysyłanego do danego kraju * Możliwość blokowania ruchu internetowego niepochodzącego lub wysyłanego do danego kraju * Możliwość blokowania ruchu poprzez podanie zakresów adresów IP i portów * Ograniczanie ruchu sieciowego (traffic shaping): * Na łączach WAN niezależnie dla każdego łącza poprzez podanie z granularnością do 1 Mb/s określonych wartości dla kierunku UP (na zewnątrz) oraz DOWN (do wewnątrz) * Na łączu komórkowym 3G/4G/LTE poprzez podanie z granularnością do 1 Kb/s określonych wartości dla kierunku UP (na zewnątrz) oraz DOWN (do wewnątrz) * Na użytkownika sieci poprzez podanie limitu z granularnością do 1 Kb/s określonych wartości dla kierunku UP (na zewnątrz) oraz DOWN (do wewnątrz) * Dla określonego ruchu aplikacyjnego w warstwie 7 określonego powyżej w punkcie 5d z granularnością do 1 Kb/s określonych wartości dla kierunku UP (na zewnątrz) oraz DOWN (do wewnątrz). Urządzenie umożliwia tworzenie do 8 reguł ograniczających ruch sieciowy, z których każda może się składać z dowolnej kombinacji aplikacji sieciowych. Dla każdej z reguł jest możliwość priorytetyzacji ruchu (wysoki priorytet, normalny priorytet, niski priorytet) oraz oznaczania ruchu danym znacznikiem DSCP (od 0 do 7) * Blokowanie stron internetowych URL zgodne z CIPA (Children's Internet Protection Act) i należących do 70 różnych kategorii w tym: narkotyki, treści dla dorosłych oraz treści pornograficzne, alkohol i tytoń, aukcje, botnety, potwierdzone i niepotwierdzone źródła spamu, strony o charakterze okultystycznym, portale randkowe, moda i uroda, usługi finansowe, hazard, gry, strony wulgarne, strony hakerskie, rasizm oraz szerzenie nienawiści, myślistwo oraz wędkarstwo, strony nielegalne, wyszukiwarki zdjęć oraz filmów, keyloggery oraz monitory stacji, źródła malware, wojskowość i militaria, oprogramowanie peer to peer, strony płatne, blogi, phishing i inne zagrożenia internetowe, serwisy umożliwiające omijanie proxy oraz anonimizację w sieci internet, wyszukiwarki, edukacja seksualna, oprogramowanie shareware oraz freeware, zakupy, social networking, spyware oraz adware, media strumieniowe, przemoc, broń, ogłoszenia sieciowe, poczta webowa * Blokowanie treści dla dorosłych w wynikach działania najpopularniejszych wyszukiwarek internetowych: Google, Yahoo, Bing – funkcja działa dla wyszukiwania niezaszyfrowanego * Blokowanie dostępu do zaszyfrowanego wyszukiwania treści internetowych w serwisie Google. * Funkcja YouTube for Schools * Możliwość definiowana własnej listy zabronionych (czarna lista) lub dozwolonych (biała lista) stron URL * Wykrywanie i ochrona przed malware * Ochrona antywirusowa i antyphishingowa * Ochrona IPS i IDS  1. Urządzenie realizuje monitoring i analizę ruchu sieciowego w zakresie:  * Wykres ilości ruchu generowanego przez wszystkich użytkowników, jednego użytkownika lub grupę użytkowników w ciągu dwóch ostatnich godzin, ostatniego dnia, ostatniego tygodnia i ostatniego miesiąca * Wykres ilości użytkowników podłączonych do sieci chronionej w ciągu dwóch ostatnich godzin, ostatniego dnia, ostatniego tygodnia i ostatniego miesiąca * Dokłada informacja, jakie aplikacje sieciowe używają użytkownicy w sieci chronionej dla wszystkich użytkowników lub dla wybranego użytkownika z podaniem wolumenu przesłanego ruchu  1. Urządzenie realizuje funkcje koncentratora VPN(dla IKEv1 oraz dla IKEv2) dla łączenia ze sobą placówek (site-to-site vpn przy użyciu tuneli IPSEC) oraz dla podłączenia urządzeń klienckich (Client VPN):  * Dla połączeń site-to-site: * obsługa trybu pracy tuneli VPN gdy cały ruch sieciowy jest tunelowany przez VPN lub trybu gdy ruch do publicznego internetu jest przesyłany bezpośrednio do internetu poza tunelem a ruch prywatny jest tunelowany * obsługa topologii gwiazdy lub pełnej siatki połączeń * konfiguracja sieci VPN typu site-to-site wymaga podania:   + Trybu pracy tuneli   + Topologii sieci VPN   + Wybrania urządzenia centralnego dla topologii gwiazdy   + Wybrania, które sieci lokalne w danej placówce mają możliwość komunikacji z siecią VPN   + Cała reszta konfiguracji sieci VPN dokonywana jest automatycznie przez oprogramowanie zarządzające i obejmuje między innymi: konfigurację tuneli VPN, konfigurację protokołów IKE/IPSec oraz wymiana kluczy i update tablic routingu, * Urządzenie posiada możliwość blokowania ruchu sieciowego na poziomie reguła warstwy 3 wymienianego pomiędzy lokalizacjami połączonymi poprzez VPN * Dla połączeń Client VPN: * obsługa protokołu L2TP dla urządzeń klienckich typu: Windows, Mac OS, IOS lub Android oraz dedykowanego klienta opartego po połączenie SSL. * Automatyczna rejestracja do dynamicznego DNS na potrzeby dostępu VPN dla Klientów (Client VPN) z możliwością zdefiniowana nazwy dla każdego z linków WAN niezależnie * Możliwość tworzenia kont na lokalnych zasobach systemu do zarządzania oraz możliwość integracji z serwerem RADIUS oraz Acrive Directory * Możliwość tworzenia tuneli IPSec do urządzeń innych producentów * Możliwość pracy w parze niezawodnościowej w trybie WARM dla potrzeb koncentracji ruchu VPN  1. Urządzenie realizuje funkcje routera do sieci Internet w zakresie:  * Fizyczne podłączenie do łącza lub łączy internetowych operatora (2 x WAN )+ interfejs USB do podłączenia modemu 3G/4G/LTE * NAT / PAT * Tryb pracy przeźroczystej (Bridge warstwy 2) * Serwer DHCP * Konfiguracja czasu dzierżawy, * Konfiguracja serwerów DNS lub użycie serwerów podanych przez nadrzędny serwer DHCP lub użycie serwerów publicznych np. Google Public DNS lub Open DNS * Konfiguracja opcji DHCP * Konfiguracja zakresów adresów zarezerwowanych lub przydzielanych statycznie * Routing statyczny IP pomiędzy sieciami VLAN (po stronie LAN) i WAN oraz pomiędzy sieciami VLAN * Wykorzystanie dwóch łączy uplinkowych WAN do sieci Internet w zakresie: * Load balancing ruchu z możliwością określenia proporcji wynikających np. z różnej prędkości łączy * Wskazanie jaki ruch sieciowy (protokół, źródłowy adres IP, źródłowy port, docelowy adres IP, docelowy port) mają zostać skierowane do którego łącza WAN * Wykorzystanie łącza nr 2 w momencie awarii łącza nr 1  1. Urządzenie zarządzane i monitorowane jest poprzez aplikację zarządzającą dostępną w chmurze. Za pomocą tej aplikacji możliwe jest zarządzanie wieloma urządzeniami danego typu np. tworzącymi VPN bez ograniczeń ilościowych w zakresie:  * Monitoring * Monitoring stanu i kondycji jednego urządzenia lub wielu urządzeń w jednym widoku * Monitoring statusu tuneli VPN w zakresie:   + Status połączenia (stan tunelu) przez ostatni dzień lub ostatni tydzień lub ostatnie 30 dni   + Ilość ruchu przesłanego przez VPN dla danej placówki przez ostatni dzień lub ostatni tydzień (sumaryczna, w relacji do innej placówki)   + Opóźnienie dla ruchu przesłanego przez VPN dla danej placówki przez ostatni dzień lub ostatni tydzień (średnie, w relacji do innej placówki) * W zakresie jednego urządzenia monitoring:   + Status urządzenia   + Numer seryjny   + Przypisane znaczniki wyszukiwania   + Adres pocztowy instalacji urządzenia   + Status interfejsów WAN wraz z przypisanymi adresami IP   + Zarejestrowana nazwa w dynamicznym DNS   + Dostęp do event loga związanego z danym urządzeniem   + Status portów LAN   + Bieżący wykres ruchu internetowego (w Kb/s lub Mb/s) odświeżany na bieżąco   + Lista stacji sieciowy dzierżawiących adresy IP przez DHCP   + Uruchomienie PING z danego urządzenia do innego urządzenia poprzez podanie nazwy hosta w Internecie, adresu IP lub adresu MAC   + Traceroute z podaniem linku WAN, który ma być użyty do wyznaczania ścieżki   + Możliwość przełączenia diod LED w tryb mrugania w celu oznaczenia urządzenia   + Możliwość restartu zdalnego urządzenia * Wysyłania alertów mailowych do wszystkich lub wybranych administratorów sieci w przypadku, gdy:   + Urządzenie jest niedostępne (offline) przez 5 lub 10 lub 15 lub 30 lub 60 minut   + Zmieni się status podstawowego łącza WAN   + Nastąpi wyczerpanie puli adresów IP serwera DHCP   + Stwierdzono konflikt adresów IP w sieci   + Zmienił się status łącza komórkowego   + Został wykryty w sieci nielegalny serwer DHCP   + W przypadku pracy urządzenia w układzie niezawodnościowym z drugim urządzeniem nastąpi wykrycie awarii i zmian ról urządzeń * Konfiguracja * Konfiguracja i uruchomienie sieci VPN site-to-site * Konfiguracja i zmiana ustawień jednego lub wielu urządzeń na raz w zakresie:   + Tryb pracy, jako router lub bridge warstwy 3   + NAT   + Routing statyczny/dynamiczny i konfiguracja sieci VLAN   + Serwer DHCP   + Filtry warstwy 3 i filtry aplikacyjne warstwy 7   + Filtry treści   + Polityki ograniczenia pasma sieciowego do poziomu reguł obejmujących kombinacje aplikacji sieciowych warstwy 7 * Konfiguracja grup użytkowników wraz z możliwością zdefiniowania dla grupy użytkowników następujących parametrów:   + Godziny i dni tygodnia dostępności lub niedostępności dostępu do sieci   + Ograniczenie pasma transmisji z granularnością do 1 Kb/s określonych wartości dla kierunku UP (na zewnątrz) oraz DOWN (do wewnątrz)   + Określenie reguł firewallingu w warstwie 3 i 7   + Określenie reguł ograniczania ruchu sieciowego (traffic shaping)   + Określenie reguł filtracji stron i treści internetowych   + Określenie listy dozwolonych i niedozwolonych adresów URL   + Uruchomienie lub wyłączenie filtrowania wyników przeszukiwania w wyszukiwarkach internetowych   + Włączenie lub wyłączenie funkcji filtrowania treści YouTube * System posiada mechanizm konfiguracji party o szablony umożliwiający łatwe instalowanie wielu urządzeń sieciowych w wielu lokalizacjach i jednoczesną zmianę parametrów konfiguracyjnych wielu urządzeń na raz * Utrzymanie: * Automatyczna aktualizacja oprogramowania jednego lub wielu urządzeń z możliwością określenia okna czasowego, kiedy taka czynność może zostać wykonana przez system zarządzający * Informowanie administratora o dostępności nowej wersji oprogramowania dla danego typu urządzenia z możliwością zablokowania automatycznego upgrade, określenia, kiedy ma być wykonany lub natychmiastowego wykonania upgrade  1. Uproszczona instalacja urządzenia, która wymaga jedynie:  * podłączenie do sieci Internet * podanie jego numeru seryjnego w systemie zarządzania i monitorowania siecią oraz * wskazanie sieci / lokalizacji, która określa jego konfigurację  1. Urządzenie obsługuje SNMP v2c oraz SYSLOG 2. Urządzenie obsługuje PPPoE dla łącza WAN 3. Dodatkowe wymagane funkcjonalności w zakresie:  * filtrowania treści * filtrowania geograficznego * ochrony IDS/IPS * Blokowania treści dla dorosłych w wynikach działania najpopularniejszych wyszukiwarek internetowych * Blokowania dostępu do zaszyfrowanego wyszukiwania treści internetowych w serwisie Google. * Funkcji YouTube for Schools * Definiowana własnej listy zabronionych (czarna lista) lub dozwolonych (biała lista) stron URL * Wykrywania i ochrony przed malware * Ochrony antywirusowej i antyphishingowej  1. Licencje dostępne muszą być dostarczone w na okres 7 lat. Licencje oprócz wyżej wymienionych funkcjonalności muszą gwarantować dostęp do chmurowego zarządzania, wsparcia producenta oraz aktualizacji oprogramowania. 2. Urządzenie objęte jest przez producenta sprzętu pełną gwarancją lifetime warranty (nie krótszą niż 5 lat). |  | |
| **2.** | **Urządzenie typu 1 - przełącznik – 2 szt.** | **Typ/model oferowanego urządzenia** |  |
| 1. Typ i liczba portów:  * 24 porty 10/100/1000BaseT RJ-45  1. Slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb):  * 8x1/10G SFP/SFP+ * 2x40G QSFP * 2x25G SFP28 * 2x(25G/10G/1G) SFP28  1. Porty SFP/SFP+/SFP28/QSFP możliwe do obsadzenia następującymi rodzajami wkładek:  * 1000BASE-SX * 1000BASE-LX10 * 1000BASE-T * 10GBASE-SR * 10GBASE-LR * 10GBASE-LRM * QSFP - MPO12 * QSFP – LC * QSFP - Duplex LC * 10GSFP+Cu(Twinax)  1. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:  * Przepustowość w ramach stosu - 480Gb/s, * 8 urządzeń w stosie, * Zarządzanie przełącznikiem poprzez dedykowany panel zarządzania w chmurze producenta. * Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad, * Możliwość współdzielenia mocy zasilaczy (grupa do 4 urządzeń w stosie) tzn. zasilacze stanowią zasób wspólny dla grupy przełączników (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania” mocy dla innych jednostek w stosie, w tym dla przełączników wymagających większej mocy dla PoE, jeśli takie są zainstalowane w stosie),  1. Zasilanie i chłodzenie:  * Redundantne i wymienne moduły wentylatorów, * Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap),  1. Parametry wydajnościowe:  * Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate): * przepustowość przełącznika (switching capacity): ] 208 Gb/s (bez podłączenia do stosu) * prędkość przesyłania (forwarding rate): 154.76 Mpps (bez podłączenia do stosu), * bufor pakietów – 16MB * Pamięć DRAM – 8GB * Pamięć flash – 16GB  1. Obsługa:  * 1000 aktywnych sieci VLAN * 32000 adresów MAC * 8192 tras IPv4 * 256 interfejsów L3 * Jumbo frame 9198B  1. Obsługa protokołu NTP 2. Obsługa IGMP/ PIM-SM//RFC4604/ 3. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:  * IEEE 802.1w Rapid Spanning Tree * Per-VLAN Rapid Spanning Tree (PVRST+) * IEEE 802.1s Multi-Instance Spanning Tree  1. Obsługa protokołu LLDP (IEEE 802.1ab) 2. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego 3. Możliwość uruchomienia funkcji serwera DHCP 4. Mechanizmy związane z bezpieczeństwem sieci:  * Wiele poziomów dostępu administracyjnego - RBAC. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu. * 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 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, * Funkcjonalność flexible authentication (możliwość wyboru uwierzytelniania – 802.1X i/lub uwierzytelnianie w oparciu o MAC adres * Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection , * Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard  1. Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:  * sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, * bezpieczna sekwencja uruchamiania, * sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia. * Mechanizmy związane z zapewnieniem jakości usług w sieci: * Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, * 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;  1. Obsługa protokołów i mechanizmów routingu:  * Routing statyczny dla IPv4 i IPv6, * Routing dynamiczny – OSPF  1. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN  * Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),  1. Parametry fizyczne:  * Możliwość montażu w szafie rack 19”, * Wysokość urządzenia 1 RU, * Głębokość chassis urządzenia z wentylatorami i zasilaczami mniejsza niż 50 cm,  1. Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników(jeśli wymaga to dodatkowej licencji nie jest to wymagane na tym etapie postępowania):  * Statycznie w oparciu o port do którego podłączona jest stacja, * Statycznie w oparciu o VLAN, w którym pracuje stacja, * Statycznie w oparciu o adres IP stacji, * Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X;  1. Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu (jeśli wymaga to dodatkowej licencji nie jest to wymagane na tym etapie postępowania), 2. Wyposażenie urządzenia  * Przełącznik wyposażony w zasilacz redundantny o mocy identyczny jak zasilacz podstawowy, * Przełącznik wyposażony jest w moduł do łączenia w stos data wraz z kablem stakującym o długości 50 cm * Przełącznik wyposażony jest w kabel o długości 30 cm umożliwiający podłączenie do grupy przełączników współdzielących energię elektryczną, * Przełącznik wyposażony jest w moduł: * 8x1/10G SFP/SFP+ * Przełącznik wyposażony jest w następujące moduły interfejsowe SFP+ pochodzące z oferty producenta przełącznika: * 10 Gigabit Ethernet typu twinax (SFP+ - SFP+) o długości 2 metrów - 12 sztuk  1. Licencje dostępne muszą być dostarczone na okres 7 lat. Licencje oprócz wyżej wymienionych funkcjonalności muszą gwarantować dostęp do chmurowego zarządzania, wsparcia producenta oraz aktualizacji oprogramowania. 2. Urządzenie zarządzane i monitorowane jest poprzez aplikację zarządzającą dostępną w chmurze. Za pomocą tej aplikacji możliwe jest zarządzanie wieloma urządzeniami danego typu. 3. Urządzenie objęte przez producenta sprzętu pełną gwarancją lifetime warranty (nie krótszą niż 5 lat). |  | |
| **3.** | **Urządzenie typu 2 – przełącznik – 6 szt.** | **Typ/model oferowanego urządzenia** |  |
| 1. Typ i liczba portów:  * 48 portów 10/100/1000BaseT RJ-45 ze wsparciem PoE/PoE+, budżet mocy dla PoE/PoE+ wymagany jest na poziomie 370W  1. Przełącznik wyposażony musi być w moduł/porty zainstalowane na stałe – 4x10G 2. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:  * Przepustowość w ramach stosu - 80Gb/s, * Do 8 jednostek w stosie  1. Wydajność przełączania min 176 Gbps 2. Obsługa:   • warstwy trzeciej L3 i routingu statycznego  • uwierzytelnienia 802.1X  • protokołu RSTP  • DHCP snooping  • Dynamic ARP Inspection  • 802.1q VLAN  • listy kontroli dostępu ACL IPv4 oraz IPv6  • QoS dla głosu i video  • Broadcast Storm Control   1. Zarządzenie oraz integracja:  * możliwość dodania lokalizacji na mapie * automatyczne umiejscowienie w topologii sieciowej L2 w systemie zarządzającym, * możliwość przygotowania konfiguracji urządzenia, zanim zostanie podłączone do sieci, urządzenie zaciągnie konfigurację automatycznie po podłączeniu. * raportowanie o odłączeniu urządzenia od sieci (e-mail). * możliwość zdalnej diagnozy problemów np. narzędzia do zdalnego przechwytywania pakietów, ping * możliwość zarządzania portami przez graficzny interfejs * statystyki ruchu na portach oraz analizy ruchu użytkowników * bezpieczne aktualizacje oprogramowania firmware z możliwością ustalenia harmonogramu  1. Wyposażenie dodatkowe: kabel zasilający oraz jeden kabel do stack o długości 1 metra 2. Wsparcie:  * dostęp do pomocy producenta 24/7, przez czas trwania licencji * usługa instalacji i konfiguracji zestawu w siedzibie zamawiającego.  1. Wbudowany zasilacz 2. Licencje dostępne muszą być dostarczone w na okres 7 lat. Licencje oprócz wyżej wymienionych funkcjonalności muszą gwarantować dostęp do chmurowego zarządzania, wsparcia producenta oraz aktualizacji oprogramowania. 3. Urządzenie zarządzane i monitorowane jest poprzez aplikację zarządzającą dostępną w chmurze. Za pomocą tej aplikacji możliwe jest zarządzanie wieloma urządzeniami danego typu. 4. Urządzenie objęte przez producenta sprzętu pełną gwarancją lifetime warranty (nie krótszą niż 5 lat). |  | |
| **4.** | **Wymogi dotyczące urządzeń sieci komputerowej** | **-** | |
| 1. W ramach realizacji umowy dostarczony sprzęt będzie posiadał gwarancję świadczoną bezpośrednio przez Producenta sprzętu. 2. W przypadku wątpliwości, podmiot sprzedający (kupujący sprzęt od partnera handlowego Producenta) ma obowiązek przedstawić oficjalny dokument Producenta, który będzie poświadczał, że sprzęt dostarczony w ramach realizacji umowy będzie sprzętem zakupionym w oficjalnym kanale sprzedaży oraz zarejestrowanym na użytkownika końcowego (kupującego sprzęt od partnera handlowego Producenta). 3. W ramach składanej oferty, Oferent zobowiązany jest do wyszczególnienia wszystkich numerów katalogowych produktów (licencje, sprzęt i oprogramowanie). 4. Zamawiający zastrzega sobie prawo sprawdzenia poprzez numery katalogowe czy dostarczony sprzęt spełnia wszystkie wyżej wymienione warunki. Lista ta na etapie oceny ofert będzie podlegała weryfikacji przez Zamawiającego lub Zamawiający może przekazać ją do weryfikacji niezależnej firmie zewnętrznej, wskazanej przez Zamawiającego, w celu weryfikacji z wymaganiami i zgodnością z SWZ. 5. W przypadku niespełnienia przez sprzęt któregokolwiek z wyżej wymienionych warunków Zamawiający zastrzega sobie prawo zwrotu całego dostarczonego sprzętu (na koszt dostawcy), jak również obciążenia dostawcy – Oferenta - karą umowną za niedotrzymanie warunków umowy. 6. Cały sprzęt musi być produkowany przez tego samego producenta. |  | |
| **Zakres konfiguracji i wdrożenia sieci** | | | |
| **1.** | **Specyfikacja prac wdrożeniowych w ramach zamówienia** | **-** | |
| 1. Przed rozpoczęciem prac należy ustalić plan adresacji i wykorzystania adresów oraz sieci logicznych VLAN. Ustalenia te będą prowadzone z wyznaczonymi do tego celu pracownikami Zamawiającego. 2. Przed rozpoczęciem prac Wykonawca musi przeprowadzić analizę stanu sieci, serwerów i jego usług oraz ustalić harmonogram prac. 3. Konfiguracja będzie obejmowała nowo dostarczone oprogramowanie i sprzęt oraz już znajdujące się urządzenia w infrastrukturze Zamawiającego. Ze względów bezpieczeństwa, szczegółowy zakres prac zostanie udostępniony tylko wyłonionemu Wykonawcy. 4. Cały sprzęt musi zostać wcześniej prekonfigurowany i sprawdzony u Wykonawcy, tak aby zminimalizować ilość prac realizowanych w siedzibie Zamawiającego. 5. W ramach prac należy również przeprowadzić rekonfigurację urządzeń, posiadanych przez Zamawiającego, do współpracy z urządzeniami dostarczonymi w ramach zamówienia jak i mechanizmami jakie zostaną uruchomione na dostarczonych urządzeniach. Sieć musi stanowić spójną całość. 6. Prace powinny zostać prowadzone w oknach serwisowych wyznaczonych przez Zamawiającego (dopuszcza się prace w godzinach wieczornych/nocnych lub w weekendy w celu minimalizacji przestoju). |  | |
| **2.** | **Usługa konfiguracji** | **-** | |
| Usługa konfiguracji dostarczonych urządzeń zawierać będzie m.in.:   1. zapewnienie łączności z 4 zdalnymi lokalizacjami przy zastosowaniu tuneli VPN site-to-site 2. konfigurację reguł ACL na urządzeniach brzegowych – ok. 10 VLAN, ok. 150 reguł ACL - docelowe ilości ACL oraz VLAN zostaną ustalone w wyniku analizy wyłonionego Wykonawcy 3. protokoły VLAN, Trunk, STP, RSTP, MSTP, LACP, adresację IP, konfigurację DNS, routingu, 4. usługa NTP, SSH, wbudowane mechanizmy RBAC oraz konta użytkowników, 5. wysyłanie zdarzeń syslog do wskazanego serwera Syslog, 6. mechanizmy bezpieczeństwa: Port Security, IP DHCP Snooping, IP Source Guard i Dynamic ARP Inspection lub w pełni równoważne, 7. hardening urządzeń sieciowych według najlepszych praktyk Producenta – wytycznych producenta sprzętu co do zasad konfiguracji, 8. personalizację ustawień do przedstawionych wymagań, 9. integrację urządzeń z obecnymi w infrastrukturze, 10. konfigurację innych funkcjonalności dostarczonych urządzeń i oprogramowania, które okażą się potrzebne w trakcie wdrożenia, gdy Wykonawca uzna zasadność ich aktywacji, 11. integrację urządzeń z systemem centralnego zarządzania i monitorowania, 12. dostosowanie powiadomień o niedostępności urządzenia lub zdarzenia na urządzeniu/porcie urządzenia, 13. przygotowanie szablonów konfiguracji dla portów dostępowych 14. integrację VPN RA z usługą Radius/Microsoft Active Directory obecnie posiadaną przez Zamawiającego. |  | |
| **3.** | **Szkolenie** | **-** | |
| Wykonawca przeprowadzi instruktaż (do 4 godzin lekcyjnych) u Zamawiającego dla 2 osób. Szkolenie ma dotyczyć zmian zaistniałych w sieci, wykorzystanych technologii, sposobu działania nowego systemu, procedur aktualizacji oprogramowania na dostarczonych urządzeniach |  | |
| **4.** | **Gwarancja** | **-** | |
| Wykonawca zobowiązany jest do zapewnienia gwarancji na wdrożoną konfigurację przez okres do 1 miesiąca po zamknięciu wdrożenia lub do momentu oddania pełnego dostępu do interfejsu zarządzającego dostarczonych urządzeń i oprogramowania. |  | |
| **5.** | **Dokumentacja** | **-** | |
| Wykonawca zobowiązany jest do udokumentowania zmian przeprowadzonych w systemie informatycznym Zamawiającego w dokumentacji powdrożeniowej. Dokumentacja ta powinna obejmować topologię oraz tabele adresacji. Wszelkie materiały i dokumentacje mają być w języku polskim. |  | |
| **6.** | **Ogólne Wymagania Rozwiązania** | **-** | |
| 1. Rozwiązanie nie może wymagać kontrolerów na miejscu ani sprzętu/oprogramowania do zarządzania jako części rozwiązania. 2. Rozwiązanie nie może mieć pojedynczego punktu awarii – wszystkie punkty dostępowe powinny działać autonomicznie w przypadku utraty połączenia z platformą zarządzania w chmurze lub Internetem. 3. Rozwiązanie musi obejmować platformę zarządzania w chmurze, która jest w pełni redundantna i zlokalizowana w kilku centrach danych. 4. Centra danych wykorzystywane przez rozwiązanie muszą mieć co najmniej 99,99% SLA, być certyfikowane zgodnie z SSAE16 i codziennie poddawane testom penetracyjnym. 5. Rozwiązanie musi oferować jednolitą platformę zarządzania („single-pane-of-glass”) do zarządzania przełącznikami, urządzeniami zabezpieczającymi, nadzorem wideo i zarządzaniem urządzeniami mobilnymi. 6. System musi umożliwiać generowanie przechwyceń pakietów za pośrednictwem konsoli zarządzania dla bezpośrednio podłączonych klientów. 7. Licencjonowanie rozwiązania powinno obejmować WSZYSTKIE obecne i WSZYSTKIE przyszłe funkcje. 8. Licencjonowanie rozwiązania powinno obejmować wsparcie 24x7. 9. Rozwiązanie musi zapewniać szczegółowe analizy ruchu sieciowego na warstwie 7. 10. Rozwiązanie musi informować administratorów, jeśli zmieni się status sprzętu lub jeśli dokonana zostanie zmiana w systemie. Dodatkowo, wszystkie zmiany w systemie muszą być rejestrowane i śledzone według użytkownika i zmienionych wartości. 11. Aplikacja zarządzająca musi obsługiwać uwierzytelnianie dwuskładnikowe. 12. Aplikacja zarządzająca musi obsługiwać wiele lokalizacji i poziomów ról administracyjnych, w tym „tylko do odczytu”, „tylko monitorowanie” 13. Rozwiązanie zarządzające musi obejmować bezpłatną aplikację mobilną do podstawowego zarządzania i raportowania, która musi działać na najnowszych platformach iOS i Android. 14. Cały sprzęt musi być produkowany przez tego samego producenta. 15. Urządzenie objęte przez producenta sprzętu pełną gwarancją lifetime warranty (nie krótszą niż 5 lat). |  | |

1. Oświadczam, że zagwarantuję pomoc techniczną przez rok od daty podpisania protokołu odbioru.
2. Oświadczam, że zapoznałem się z treścią zapytania ofertowego oraz że nie wnoszę zastrzeżeń do jego treści i zdobyłem wszelkie informacje niezbędne do sporządzenia oferty i wykonania zamówienia.
3. Oświadczam, że akceptuję termin związania ofertą wynoszący 30 dni od dnia upływu terminu składania ofert, przy czym pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert.
4. Zobowiązuje się wykonać zamówienie w terminach wskazanych w Zapytaniu ofertowym.
5. W przypadku wyboru mojej oferty zobowiązuję się do zawarcia umowy na wykonanie przedmiotu zamówienia w miejscu i terminie wskazanym przez Zamawiającego.
6. Umowa będzie opiewać na kwotę brutto.
7. Znajduję się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.
8. Posiadam wiedzę i doświadczenie niezbędne do realizacji przedmiotu zamówienia.
9. Wyrażam zgodę na przetwarzanie przez Zamawiającego danych osobowych na potrzeby realizacji niniejszego postępowania zgodnie z art. 23 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 ze zm.) do celów związanych z przeprowadzeniem niniejszego postępowania. Moja zgoda obejmuje również przetwarzanie danych w przyszłości pod warunkiem, że nie zostanie zmieniony cel przetwarzania.
10. Jestem świadomy/-a odpowiedzialności karnej za fałszywe zeznania wynikające z art. 233 (podanie nieprawdy lub zatajenie nieprawdy) ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r., Nr 88, poz. 553 ze zm.), a zawarte w ofercie informacje są zgodne z prawdą oraz stanem faktycznym.

………….……………………………

Czytelny podpis osoby uprawnionej do reprezentowania podmiotu

Załączniki:

1. Załącznik nr 2 – Oświadczenie Wykonawcy – warunki udziału w postępowaniu
2. Załącznik nr 3 – Wykaz dostaw
3. Załącznik nr 4 – Wykaz personelu
4. Certyfikaty techniczne producenta oferowanych urządzeń
5. Referencje/protokoły potwierdzające prawidłowość wykonania dostaw
6. Wykaz numerów katalogowych produktów (licencje, sprzęt i oprogramowanie).

1. Zakres danych i informacji musi także potwierdzać **równoważność** oferowanych urządzeń, w stosunku do wymagań wskazanych przez Zamawiającego [↑](#footnote-ref-1)