Router I centrala 1 szt.*

Wykonawca wypełnia poniższą tabelę w przypadku gdy zaoferowany przez Wykonawcę sprzęt nie będzie kompatybilny z posiadanym przez Zamawiającego Routerem centralnym Cisco ASR1001X . W sytuacji zaoferowania przez Wykonawcę sprzętu kompatybilnego z ww routerem kol. nr 4 należy pozostawić niewypełnioną.

Oferowany model (w tym karty rozszerzeń, moduły, licencje, numery katalogowe): ..... producent: .....

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
1.	Wymagania	Urządzenie o architekturze modularnej, wyposażone w co najmniej 6 portów Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP. W chwili dostarczenia urządzenia zamawiający wymaga dostarczenia urządzenia z dostępnymi i aktywnymi 4 portami 1000BASE-T oraz 2 portami 1000BASE SX-MM, urządzenie musi umożliwiać rozbudowę o min. 2 porty 10 Gigabit Ethernet	
		Urządzenie musi umożliwiać rozszerzenie m.in. o następujące porty: a) 1 port 10 GigabitEthernet b) 8 portów Gigabit Ethernet	
		Musi posiadać zasoby sprzętowe zapewniające wydajność przełączania min. 19 Mpps oraz min. 15 Gbps ruchu	
		Musi posiadać wydajność szyfrowania min. 5,5 Gbps dla ruchu IMIX (encryption+decryption).	
		Musi być wyposażone w minimum 4 GB pamięci RAM.	
		Obsługa minimum 800 000 prefiksów w tablicach rutingu dla IPv4.	
		Obsługa minimum 150 000 prefiksów w tablicach rutingu dla IPv6.	
		Musi obsługiwać następujące protokoły routingu dynamicznego dla IPv4: OSPF, ISIS, BGP.	
		Musi obsługiwać następujące protokoły routingu dynamicznego dla IPv6: OSPFv3, ISIS, BGP.	
		Obsługa Policy Based Routing, w tym także routing oparty o pomiar parametrów łącza	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		(opóźnienie, obciążenie, jitter) z możliwością definiowania polityk per aplikacja.	
		Urządzenie musi umożliwiać uruchomienie wydzielonych wirtualnych instancji (przestrzeni) routingowych w oparciu o mechanizm VRF (Virtual Routingu Forwarding), umożliwiając m.in. wykreowanie wydzielonej logicznej sieci na potrzebę obsługi ruchu określonej aplikacji lub wydzielonego fragmentu sieci.	
		Musi obsługiwać 500 instancji wirtualnych tablic routingu.	
		Musi obsługiwać funkcjonalność Bidirectional Forwarding Detection (BFD), zapewniając przy tym wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego.	
		Musi obsługiwać funkcjonalność BFD dla interfejsów skonfigurowanych do współpracy z VRF.	
		Musi obsługiwać multicast, w szczególności: PIM sparse/dense/SSM, IGMP, Multicast VPN.	
		Musi obsługiwać protokół NHRP (ang. Next Hop Resolution Protocol)	
		Urządzenie musi posiadać następujące funkcjonalności związane z niezawodnością pracy: a) BFD dla OSPF, BGP, ISIS b) IP FRR c) Graceful Restart dla OSPF, BGP, ISIS, d) funkcjonalność VRRP lub równoważny e) redundantne zasilacze AC 230V zintegrowane w obudowie urządzenia f) możliwość wymiany modułów w trakcie pracy (ang. hot swap)	
		Urządzenie musi obsługiwać MPLS, w	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		szczególności: a) LDP b) MPLS L2 VPN, VPLS c) MPLS L3 VPN d) MPLS TE e) MPLS FRR w trybach protekcji łącza oraz węzła	
		Urządzenie musi obsługiwać następujące mechanizmy jakości usług (QoS): a) klasyfikacja, kolejkowanie, oznaczanie, policing, shaping per port/VLAN dla kart L2, zarówno dla IPv4 jak i IPv6 b) hierarchiczny QoS (H-QoS) - 3 poziomy c) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: adres MAC, adres IP, port TCP, VLAN ID, MPLS EXP, 802.1p (CoS), IP ToS/DSCP. d) dynamiczna alokacja kolejek sprzętowych, dostępne min. 16 000 kolejek e) algorytm Round Robin (Shaped Round Robin) dla obsługi kolejek lub równoważny f) możliwość obsługi jednej kolejki z priorytetem w stosunku do innych g) możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP h) możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi (ingress policing, rate limiting) i) mechanizm WRED j) możliwość wykorzystania rodzajów aplikacji/ruchu aplikacyjnego w tworzeniu polityk QoS	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Urządzenie musi obsługiwać następujące funkcje i elementy bezpieczeństwa: a) ochrona warstwy zarządzającej (Control Plane Policing), ze wsparciem dla list kontroli dostępu b) Unicast RPF (Reverse Path Forwarding) c) listy kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, flagi TCP, d) min. 30 000 wpisów IPv4 na wszystkich listach kontroli dostępu (ACL), e) dostęp administracyjny oparty o role z przypisanymi uprawnieniami f) urządzenie ma realizować funkcjonalności zapory ogniowej typu statefull (ang. statefull firewall), przy czym zapora ogniowa: • umożliwia definicję stref bezpieczeństwa (zone-based firewall) z elastyczną definicją scenariuszy przesyłu ruchu pomiędzy różnymi strefami (inspekcja ruchu, odrzucanie ruchu, brak inspekcji). • obsługuje ruch IPv4 oraz IPv6 • umożliwia konfigurację polityk per wirtualna tablica routingu (VRF) • umożliwia obsługę 2 000 000 równoczesnych sesji • umożliwia zestawienie 200 000 nowych połączeń TCP na sekundę g) zasoby sprzętowe realizujące funkcjonalności szyfrowania VPN z wydajnością min. 5,5 Gbps (AES256+SHA512) (encryption+decryption), h) sieci VPN typu site-2-site oparte o IPSec i) dynamiczne zestawianie VPN z wykorzystaniem protokołu NHRP (lub równoważny) w relacji spoke to spoke w celu optymalizacji transmsji danych	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		pomiędzy oddziałami. j) bez-tunelowe sieci VPN w relacji każdy z każdym w celu zapewnienia optymalnej transmisji pomiędzy dowolnymi węzłami oraz optymalnej realizacji polityk jakości usług (QoS) i transmisji multicast	
		Musi obsługiwać bezpieczne algorytmy IPSec, w szczególności: a) Elliptic Curve Diffie-Hellman (ECDH) z modulo Prime 521-bit b) Diffie-Hellman, z kluczem 2048 bitów c) Advanced Encryption Standard (AES), z kluczem 256 bitów d) RSA, z kluczem 4096 bitów e) SHA2, z kluczem 512 bitów	
		Konfigurację tuneli IPSec VPN w oparciu o protokół IKEv2 a) IKEv2 dla VPN typu site-2-site b) IKEv2 zarówno dla ruchu IPv4 jak i IPv6	
		funkcjonalność VPN per VRF	
		ochronę centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU	
		Urządzenie musi wspierać usługi klasyfikacji ruchu w oparciu o głęboką analizę pakietów, klasyfikacja ta powinna udostępniać co najmniej 3 atrybuty opisujące daną aplikację/protokół atrybuty mają ułatwić konfigurowanie QoS na urządzeniu poprzez grupowanie podobnych aplikacji/protokołów (na przykład wszystkie aplikacje typu p2p mają taką samą wartość atrybutu określającego typ aplikacji). Włączenie usługi nie może powodować konieczności rozbudowy sprzętowej urządzenia, co najwyżej zakup licencji pozwalającej na korzystanie z powyższej funkcjonalności.	
		Urządzenie musi obsługiwać zestawianie tuneli GRE.	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Urządzenie musi posiadać możliwość tunelowania przesyłanych danych w postaci tuneli GRE typu punkt-punkt z możliwością uruchomienia protokołów routingu dynamicznego pomiędzy urządzeniami połączonymi za pomocą tuneli GRE.	
		Urządzenie musi umożliwiać ochronę kryptograficzną tuneli GRE.	
		W ramach funkcjonalności zarządzania, urządzenie musi: a) umożliwiać zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3 b) obsługiwać język skryptowy c) obsługiwać protokół Netflow lub Netstream lub równoważny d) posiadać narzędzia IP SLA umożliwiające pomiar parametrów jakościowych łącza (np. czas odpowiedzi aplikacji/serwera, opóźnienie, jitter, straty pakietów) i dostęp do tych informacji za pomocą SNMP e) posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania z wykorzystaniem protokołów RADIUS lub TACACS+ f) posiadać dedykowane porty do zarządzania urządzeniem: port konsoli (RJ45), port Ethernet g) posiadać port USB h) posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona i) posiadać możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Urządzenie musi umożliwiać montaż w szafie 19".	
		Musi być wykonane z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.	

Routery 25 szt.

Oferowany model (w tym karty rozszerzeń, moduły, licencje, numery katalogowe): .....

producent: .....

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
1.	Wymagania	Musi być urządzeniem pełniącym rolę wielousługowego routera modularnego gotowego do obsługi mechanizmów bezpiecznej i niezawodnej sieci WAN w oparciu o Internet oraz MPLS	
		Musi pozwalać na instalację co najmniej: jednego modułu rozszerzeń takich jak moduły przełącznika, 2 kart z interfejsami sieciowymi	
		Musi posiadać zintegrowaną sprzętową akceleracje szyfrowania DES/3DES/AES	
		Musi posiadać wszystkie interfejsy „aktywne". Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów.	
		Sloty urządzenia przewidziane pod rozbudowę muszą mieć możliwość obsadzenia modułami: z interfejsami szeregowymi WAN, przełącznika Ethernet (funkcje L2 i L3), oczekiwana liczba portów przełącznika nie może być mniejsza niż 8 dla jednego modułu; z portem VDSL2 / ADSL2+ over POTS / Annex M;	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Urządzenie musi oferować możliwość zwiększenia wydajności do co najmniej 300Mbps dla ruchu IMIX bez rozbudowy o dodatkowe moduły sprzętowe – np. licencyjnie przez odblokowanie wbudowanych zasobów sprzętowych lub jako większa wydajność początkowa routera;	
		Urządzenie musi oferować dla pakietów IMIX przy włączonych usługach szyfrowania z IPSec, szczegółowej analizy aplikacji, kontroli jakości usługi QoS o przepustowość minimum 200Mbps;	
		Musi posiadać obsługę protokołów routingu IP BGPv4, OSPFv3, IS-IS, RIPv2 oraz routingu multicastowego PIM (Sparse i SSM) oraz routing statyczny;	
		Protokół BGP musi posiadać obsługę 4 bajtowych ASN;	
		Musi posiadać wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMP v1/v2, IGMP Snooping, PIMv2, Bi-directional PIM;	
		Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF)	
		Musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q, urządzenie musi obsługiwać co najmniej 1000 sieci VLAN	
		Musi obsługiwać IPv6 w tym ICMP dla IPv6	
		Musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, flagi TCP	
		Urządzenie musi posiadać wbudowany mechanizm logowania zdarzeń systemowych a także liczników pokazujących ilość pakietów i bajtów odrzuconych/przepuszczonych przez wybraną regułę listy kontroli dostępu. Musi istnieć możliwość wysyłania logów systemowych na zewnętrzny serwer.	
		Musi posiadać obsługę NAT dla ruchu IP unicast oraz PAT dla ruchu IP unicast	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Mechanizm NAT musi zapewniać wsparcie dla H.245 lub SIP	
		Musi posiadać obsługę wirtualnych instancji routingu (VRF) - co najmniej 64 instancji VRF	
		Musi posiadać obsługę mechanizmu DiffServ	
		Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu.	
		Musi zapewniać obsługę mechanizmów kolejkowania ruchu: z obsługą kolejki absolutnego priorytetu ze statyczną alokacją pasma dla typu ruchu WFQ	
		Musi obsługiwać mechanizm WRED	
		Musi obsługiwać mechanizm Traffic Shaping	
		Musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu	
		Musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precendence dla ruchu tunelowanego.	
		Musi obsługiwać protokół NTP	
		Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP lub GLBP lub VRRP)	
		Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+	
		Musi obsługiwać protokół MPLS (funkcje LER i LSR)	
		Musi obsługiwać MPLS over GRE	
		Musi wspierać QoS dla MPLS	
		Musi obsługiwać MPLS Traffic Engineering	
		Musi obsługiwać MPLS L2 i L3 VPN oraz VPLS	
		Musi obsługiwać funkcjonalność Bidirectional Forwarding Detection (BFD)	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		lub równoważna	
		Funkcjonalność BFD musi być dostępna dla intefejsów skonfigurowanych do współpracy z VRF	
		Musi obsługiwać funkcjonalność BFD Echo Mode lub równoważna	
		Funkcjonalność BFD (lub równoważna) musi posiadać wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego oraz HSRP lub VRRP lub równoważne.	
		Musi posiadać funkcjonalność pozwalającą na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy (np. Embedded Event Manager – EEM lub Tcl lub równoważny)	
		Funkcjonalność EEM lub równoważna musi pozwalać na generowanie akcji: a. Wykonanie komendy z poziomu linii poleceń urządzenia b. Wysłanie krótkiej wiadomości tekstowej poprzez system poczty elektronicznej c. Wykonanie skryptu d. Wygenerowanie SNMP trap	
		Musi posiadać możliwość sterowania ruchem wyjściowym, niezależnie od tablicy routingu, poprzez wskazanie routera docelowego (next-hop) dla konkretnego ruchu, określonego adresami/podsieciami źródłowymi i docelowymi. Musi istnieć możliwość takiej konfiguracji, żeby powyższa polityka kierowania konkretnego ruchu na konkretny router przestała automatycznie obowiązywać kiedy router docelowy przestaje być osiągalny (przestaje odpowiadać na zawołanie ICMP-echo wysłane z konkretnego interfejsu lub IP źródłowego). W takim przypadku ruch powinien zostać obsłużony zgodnie z tablicą routingu.	
		Urządzenie musi posiadać możliwość integracji z centralnym systemem	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		zarządzania, monitorowania, konfiguracji jak również troubleshootingu	
		Urządzenie musi umożliwiać obsługę przez zcentralizowany system zarządzania w celu zmiany wersji systemu operacyjnego.	
		Musi oferować zaawansowane funkcjonalności bezpieczeństwa takie jak: a) Filtr pakietów oparty o strefy bezpieczeństwa (np. Zone Based Firewall ZBF lub równoważny), b) IPSec VPN, c) Dynamiczny VPN oparty o otwarte protokoły NHRP i mGRE (Dynamic Multipoint VPN DMVPN lub Dynamic Smart VPN lub równoważny).	
		Musi obsługiwać bezpieczne algorytmy IPSec, w szczególności: a) Elliptic Curve Diffie-Hellman (ECDH) z modulo Prime 521-bit b) Diffie-Hellman, z kluczem 2048 bitów c) Advanced Encryption Standard (AES), z kluczem 256 bitów d) RSA, z kluczem 4096 bitów e) SHA2, z kluczem 512 bitów	
		Musi posiadać funkcjonalność sterowania ruchem i jego rozkładu na łącza różnych operatorów na bazie konfigurowalnych polityk uwzględniających SLA (np. dopuszczalny poziom strat w pakietach, bajtach, dopuszczalne opóźnienia, dopuszczalna zmienność opóźnień - tzw. "jitter").	
		Musi być zarządzalne za pomocą SNMPv3	
		Urządzenie musi umożliwiać identyfikowanie aplikacji oraz w ich oparciu budować polityki QoS.	
		Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Netflow lub JFlow lub równoważnego	
		Musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI) jak również interfejsu graficznego (GUI)	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.	
		Musi być wykonana z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej	
		Musi mieć możliwość montażu w szafie 19" i musi zostać dostarczone z umożliwiającym to zestawem montażowy	
		Urządzenie musi posiadać wbudowany zasilacz umożliwiający zasilanie prądem przemiennym 230V	
		Urządzenie musi być wyposażone w minimum 2 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci WAN/LAN	
		Urządzenie musi być wyposażone w minimum 3 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci WAN/LAN. W chwili dostarczenia urządzenie musi posiadać aktywne minimum 3 interfejsy z portami 1000BASE-T	
		Urządzenie musi być wyposażone w minimum 512MB pamięci Flash	
		Urządzenie musi być wyposażone w minimum 1GB pamięci RAM	
		Urządzenie musi być wyposażone w minimum jeden port USB. Port musi	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych.	
		Urządzenie musi być wyposażone w port konsolowy szeregowy RJ45 i USB	
		Urządzenie musi być dostarczone z kablami pozwalającymi na podłączenie zarówno konsoli USB jak i szeregowej, jak również kablami zasilającymi.	

System zarządzania

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
1.	Wymagania	zarządzanie i zbieranie statystyk z wykorzystaniem co najmniej SNMP	
		narzędzia automatycznej identyfikacji i wyszukiwania urządzeń instalowanych w sieci: możliwość manualnego dodawania urządzeń oraz automatycznego za pośrednictwem protokołów takich jak: LLDP,	
		narzędzia wyświetlania urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu	
		mapa topologii urządzeń z połączeniami oraz wizualizacja alarmów na urządzeniach	
		narzędzia do konfiguracji urządzeń w zakresie przynajmniej interfejsów, list kontroli dostępu, wybranych protokołów routingu na routerach	
		wbudowane przykładowe wzorce konfiguracji urządzeń, takie jak: konfiguracja usług bezpieczeństwa, agregacji linków, konfiguracji NTP, SNMP, NAT, itp.	
		narzędzie do tworzenia wzorców konfiguracji na urządzenia	
		funkcje archiwizacji konfiguracji, przeglądania zmian konfiguracji, automatyzacji zbierania konfiguracji urządzeń	
		narzędzie do przeprowadzenia inwentaryzacji komponentów używanych w sieci w tym sprzętu i oprogramowania systemowego urządzeń sieciowych	
		narzędzie do zarządzania obrazami oprogramowania urządzeń	
		narzędzie umożliwiające zbieranie informacji o parametrach urządzeń, przynajmniej takich jak: zajętość CPU, zajętość pamięci, dostępność, ilość portów, utylizacja portów, itp.	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		zbieranie statystyk z urządzeń sieciowych za pomocą Netflow lub równoważnego	
		monitoring wydajności sieci wraz z możliwością zbierania informacji o aplikacjach w sieci i parametrach ich działania pozwalające na analizę (np.: ilość ruchu, czas odpowiedzi, czas transakcji oraz opóźnienie)	
		monitoring, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie	
		narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku	
		narzędzie do zbierania alarmów pochodzących z urządzeń, kategoryzacji alarmów	
		informowanie o alarmach/incydentach przez notyfikację email	
		narzędzie do konfiguracji, monitoringu (technologia VPN, polityka routingu oraz polityka QoS z podziałem na aplikacje)	
		praca w trybie przeglądarkowym pozwalając administratorowi na dostęp z dowolnego (po uzyskaniu odpowiednich uprawnień) miejsca w sieci	
		budowanie widoków przez użytkownika	
		hierarchizacja zarządzania – możliwość określenia domen administracyjnych dla administratorów, możliwość wykorzystania wbudowanej bazy administratorów lub zewnętrznego serera uwierzytelniającego	
		narzędzia pozwalające na podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy	
		współpraca z serwerami czasu (NTP)	
		wbudowane formularze do konfiguracji usług na nowych urządzeniach	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		wbudowane formularze do weryfikacji możliwości urządzeń pod kątem uruchomienia nowych usług (np. IEEE 802.1X)	
		narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku	
		tworzenie raportów dotyczących urządzeń sieciowych, urządzeń klienckich oraz wydajności sieci	
		narzędzie pozwalające na monitoring wydajności sieci wraz z możliwością zbierania informacji o aplikacjach w sieci i parametrach ich działania, pozwalające na analizę, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie, itp.	
		narzędzie pozwalające na diagnostykę działania urządzenia przez wykonanie ping, traceroute, połączenie się z urządzeniem przez telnet, ssh, http, https	
		narzędzie pozwalające na analizę połączenia urządzeń klienckich i użytkowników podłączonych w sposób przewodowy do infrastruktury; narzędzie powinno pozwalać na m.in.: zbieranie informacji o parametrach podłączenia i umożliwiać administratorowi szybką analizę problemów związanych z podłączeniem urządzenia do infrastruktury	
		API REST do integracji z innymi narzędziami/systemami	
		dostarczona wersja musi posiadać licencje na zarządzanie urządzeniami będącymi przedmiotem przetargu z możliwością rozbudowy do przynajmniej 300, ponadto musi umożliwiać dostęp oraz prawo do użytkowania nowych wersji oprogramowania, przez min. 3 lata.	
		system zarządzania musi pochodzić od producenta dostarczonego sprzętu.	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		system musi być dostarczony w najnowszej dostępnej wersji	
		wspiera wysoką dostępność i pracę w trybie active-standby, (nie wymaga się dostarczania systemu w wysokiej dostępności)	
		umożliwia synchronizację danych między systemami redundantnymi	
		instalacja w formie maszyny wirtualnej lub na serwerach fizycznych wspieranych przez producenta systemu	
		wymaga się dostarczenia w formie maszyny wirtualnej pracującej pod VMware ESXi	
		Zamawiający nie wymaga dostarczenia platformy sprzętowej pod system do zarządzania.	

System uwierzytelnienia

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
1.	Podstawowe cechy systemu	System musi umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych.	
		System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji dla bazowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych.	
		System musi umożliwiać wsparcie co najmniej 5 000 urządzeń końcowych dołączonych do sieci oraz zapewniać skalowalność do przynajmniej 10 000 urządzeń poprzez rozbudowę istniejącego wdrożenia.	
		System musi zostać dostarczony w formie maszyny wirtualnej.	
		System powinien umożliwiać instalację na maszynie wirtualnej (VM) i maszynie fizycznej, w tym: a) na hypervisorze VMWare ESXi 5.x i 6.x b) na hypervisorze VMware vSphere Client 5.x and 6.x c) na serwerach fizycznych	
		System musi umożliwiać wydzielenie określonych elementów funkcjonalnych, instalowanych jako oddzielne maszyny fizyczne lub wirtualne, w tym na podsystem zarządzania oraz podsystem usługowy.	
		System musi zapewniać realizację wysokiej dostępności elementów funkcjonalnych, w tym: a) zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu b) zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych	
		System musi umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych – co najmniej przez serwer TFTP, serwer FTP/SFTP, serwer HTTP/HTTPS, udział NFS	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		System musi umożliwiać zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).	
		System musi umożliwiać tworzenie kopii zapasowej na życzenie i w regularnych odstępach czasowych.	
		System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.	
		System musi umożliwiać wymuszenie reguł złożoności haseł dla administratorów, w tym co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. System musi wymuszać hasło różne od trzech poprzednich haseł i jego zmianę co określoną ilość dni	
		System musi umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora: a) dostęp do interfejsu konfiguracji usług tożsamości 802.1X b) dostęp do interfejsu konfiguracji urządzeń sieciowych c) dostęp do interfejsu konfiguracji polityk d) dostęp do interfejsu konfiguracji kontroli dostępu gościnnego e) dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania	
		System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.	
2.	Mechanizmy uwierzytelniania 802.1x	System musi wspierać następujące protokoły uwierzytelniania i standardy: a) RADIUS, zgodnie z dokumentami: i. RFC 2138 — Remote Authentication Dial In User Service (RADIUS) ii. RFC 2139 — RADIUS Accounting iii. RFC 2865 — Remote Authentication Dial In User Service (RADIUS) iv. RFC 2866 — RADIUS Accounting v. RFC 2867 — RADIUS Accounting for Tunnel Protocol Support vi. RFC 2868 — RADIUS Attributes for Tunnel Protocol Support vii. RFC 2869 — RADIUS Extensions	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		b) RADIUS Proxy dla zewnętrznego serwera RADIUS	
		System musi wspierać protokół Windows Active Directory, w tym co najmniej następujące repozytoria AD: a) Microsoft Windows Active Directory 2008 32bit i 64bit b) Microsoft Windows Active Directory 2008 R2 64bit c) Microsoft Windows Active Directory 2012 d) Microsoft Windows Active Directory 2012 R2	
		System musi wspierać serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865	
		System musi wspierać następujące protokoły uwierzytelniania: a) PAP/ASCII b) CHAP c) MS-CHAPv1 d) MS-CHAPv2 e) EAP-MD5 f) EAP-TLS g) Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi: i. EAP-MS-CHAPv2 ii. EAP-GTC iii. EAP-TLS h) System musi umożliwiać konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect	
		System musi wspierać implementację 802.1X z przynajmniej następującymi suplikantami: a) wbudowanym klientem 802.1X dla Windows 7, 8, 8.1, 10 b) Apple Mac OS X Supplicant c) Apple iOS Supplicant d) Google Android Supplicant	
		System musi umożliwiać tworzenie polityk uwierzytelniania 802.1X opartych o złożone reguły (rule-based).	
		System musi umożliwiać uwierzytelnianie 802.1X maszyn i użytkowników.	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		System musi umożliwiać tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o reguły.	
		System musi posiadać lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym)	
		System musi posiadać lokalną bazę stacji końcowych. Lokalna baza stacji końcowych musi być tworzona per stacja końcowa na podstawie unikalnego adresu MAC.	
		System musi wspierać uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC	
		System musi wspierać zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices), w tym: a) tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host per port b) tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia c) tryb uwierzytelniania 802.1X dozwalający wiele hostów na jednym porcie fizycznym d) mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny e) mechanizm umożliwiający wysłanie informacji o reloadzie urządzenia (przełącznika) dostępowego do serwera AAA. Dzięki temu uwierzytelnione aktywne sesje związane z tym konkretnym urządzeniem zostaną usunięte z listy na serwerze AAA. f) mechanizm przypisania VLANu w procesie uwierzytelnienia i kontroli dostępu 802.1X g) mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1X h) obsługa przypisania listy kontroli	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki i) mechanizm 802.1x umożliwiający realizację dostępu gościnnego w dedykowanym VLANie (Guest VLAN) dla użytkowników gościnnych j) współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN k) możliwość elastycznej konfiguracji kolejności metod 802.1X użytych do uwierzytelnienia stacji, w tym uwierzytelnienia względem centralnej bazy MAC, metod EAP dla 802.1X i uwierzytelnienia web l) możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego, jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznika	
		System musi wspierać uwierzytelnianie nazwą użytkownika i hasłem przez portal web, jako jedną z metod uwierzytelniania do sieci, (dotyczy m.in. w sytuacji, gdy stacja ma niepoprawnie skonfigurowane lub niedziałające oprogramowanie suplikanta 802.1X)	
		System wspiera przynajmniej następujące urządzenia sieciowe, jako klientów RADIUS (NAD - Network Access Device): Przełączniki sieciowe: Cisco WS-C2960S-48FPD-L Cisco WS-C2960S-24TS-L Cisco WS-C6509-E (M8572) Cisco WS-3850-48P-L Cisco WS-3650-48FD-L	
		System musi zawierać funkcjonalność serwera TACACS+ lub równoważny do administrowania urządzeniami sieciowymi bez konieczności rozbudowy sprzętowej	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
3.	Dostęp gościnny	System musi umożliwiać realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, co najmniej dla: a) Microsoft Windows 10, Windows 8.1, Windows 8, Windows 7 b) Apple Mac OS X 10.x c) Apple iOS 8.0, 7.x, 6.1, 6, 5.1, 5.0.1 d) Google Android dla 2.2 i nowszych e) Linux	
		System musi umożliwiać dodawanie kont gościnnych przez wybrane osoby (sponsor).	
		System musi zapewniać uwierzytelnienie sponsora które musi odbywać sekwencyjnie się w oparciu o: a) wewnętrzną bazę użytkowników b) zewnętrzne repozytorium użytkowników	
		System musi umożliwiać konfigurację uprawnień sponsora, w tym uprawnienia do: a) logowania się do systemu b) tworzenia pojedynczego konta gościnnego c) tworzenia wielu kont gościnnych d) importowania kont gościnnych z pliku CSV e) wysyłania wiadomości email po utworzeniu konta gościnnego f) wysyłania wiadomości SMS po utworzeniu konta gościnnego g) wyświetlenia hasła konta gościnnego h) wydrukowania danych konta gościnnego i) wyświetlenia danych stworzonych kont gościnnych j) zawieszenia (suspend) i reinicjacji kont gościnnych	
		System musi umożliwiać personalizację wyglądu portalu sponsora i gościa, w tym: a) zmianę logo strony logowania b) zmianę obrazu tła strony logowania c) zmianę logo bannera d) zmianę obrazu tła bannera e) zmianę koloru tła strony z treścią	
		System musi umożliwiać automatyczne kasowanie wygasłych kont gościnnych: na żądanie i okresowo co zadaną liczbę dni i o określonej godzinie.	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		System musi posiadać wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim, angielskim,	
		System musi umożliwiać stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim.	
		System musi umożliwiać wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora: a) Imienia b) Nazwiska c) Firmy d) adresu e-mail e) numeru telefonu f) danych opcjonalnych	
		System musi umożliwiać konfigurację dla użytkowników gościnnych: a) wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP) b) zezwolenia gościom na zmianę hasła c) samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora	
		System musi umożliwiać honorowanie ustawień local przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego.	
		System musi umożliwiać konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego.	
		System musi umożliwiać konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługiwać co najmniej 6 urządzeń per konto gościnne.	
		System musi umożliwiać konfigurację czasu ważności hasła w dniach w przedziale zadanym przedziale w dniach.	
		System musi umożliwiać określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny	
		System musi umożliwiać konfigurację polityki złożoności haseł użytkowników gościnnych	
		System musi umożliwiać konfigurację polityki nazwy (login) użytkownika	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		gościnnego w tym co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika	
		System musi umożliwiać tworzenie portalu gościnnego bez konieczności uwierzytelniania się gościa nazwą użytkownika i hasłem z opcjonalną akceptacją AUP (Acceptable Use Policy) i z koniecznością podania kodu dostępu.	
		System musi umożliwiać przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsu IP, portu HTTPS i certyfikatu SSL dla FQDN.	
		System musi umożliwiać udostepnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP i poprzez SMS,	
		System musi wspierać API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych.	
4.	Profilowanie urządzeń	System musi umożliwiać dokonanie profilowania (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu.	
		System musi umożliwiać wykorzystanie danych z procesu profilowania do zdefiniowania polityk bezpieczeństwa. W szczególności musi zapewniać stworzenie polityk np. dla wszystkich drukarek, dla wszystkich urządzeń mobilnych, dla wszystkich stacji z Windows, etc.	
		System musi umożliwiać dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł: a) DHCP b) http c) RADIUS d) DNS e) SNMP f) Network Scan (NMAP lub inne narzędzie profilowania aktywnego)	
		System musi umożliwiać wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji.	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		System musi umożliwiać dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy.	
		System musi posiadać dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla: a) Stacji roboczych pracujących z systemami Linux, Macintosh, Microsoft Windows, b) Urządzeń mobilnych: Android, Apple, Blackberry c) Drukarek sieciowych d) Routerów	
		System musi umożliwiać subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, w tym następujących informacji: a) reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci b) reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie http://standards.ieee.org/develop/regauth/oui/oui.txt	
		System musi umożliwiać włączenie funkcjonalności regularnej (z częstotliwością dobową) i automatycznej subskrypcji nowych profili urządzeń ze strony producenta o zadanej godzinie lub jej całkowite wyłączenie w dowolnym momencie.	
		System musi wspierać raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta.	
5.	Analiza stacji końcowej (Posture Assessment)	System umożliwia pobranie bazy wiedzy reguł analizy stacji końcowej (Posture) dla wspieranych systemów Antywirusowych (AV) i Antispyware (AS) ze strony producenta.	
		System umożliwia kontrolę zachowania dla stacji końcowych, które nie posiadają zainstalowanego agenta głębokiej analizy stacji końcowej (Posture).	
		System umożliwia regularne ponawianie głębokiej analizy stacji końcowej (periodic	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		reassessment) w przedziale od 1 do 24 godzin.	
		System umożliwia przedstawienie użytkownikowi dokumentu Polityki Akceptowalnego Użycia (AUP). Polityka AUP jest prezentowana w postaci strony web po procesie głębokiej analizy stacji. Zawartość dokumentu AUP jest konfigurowalna.	
		System umożliwia głęboką analizę stacji końcowej Windows pod kątem plików (File Condition), w tym: a) istnienia pliku na stacji końcowej b) wersji pliku na stacji końcowej (równa, wcześniejsza niż, późniejsza niż) c) daty utworzenia i modyfikacji pliku na stacji końcowej (równa,	
		d) wcześniej niż, później niż)	
		System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, 10 pod kątem wpisów w rejestrze (Registry Condition), w tym: kluczy rejestru z kluczem root: HKCR, HKCU, HKLM, HKU, HKCC z zadanym podkluczem pod kątem: a) istnienia lub nieistnienia klucza b) wartości klucza rejestru c) istnienia i wartości domyślnej wartości klucza rejestru typu Number, String, Version	
		System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, 10, pod kątem uruchomionych aplikacji (Application Condition), w tym: a) nazwy uruchomionego lub nieuruchomionego procesu	
		System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, 10, pod kątem uruchomionych usług systemowych (Service Condition), w tym: a) nazwy uruchomionej lub nieuruchomionej procesu	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		System umożliwia tworzenie słownika prostych i złożonych warunków (Simple i Compound Condition) dla głębokiej analizy stacji końcowej za pomocą wyrażeń logicznych AND, OR, NOT, w tym z uwzględnieniem: a) parametrów dostępu do sieci, w tym: b) lokalizacji stacji końcowej c) nazwy użytkownika d) adresu IP stacji e) metody uwierzytelnienia f) statusu uwierzytelnienia g) repozytorium użytkowników użytych dla uwierzytelnienia h) atrybutów RADIUS, w tym: i. Calling-Station-ID ii. Framed-IP-Address iii. NAS-Identifier i) NAS-IP-Address j) NAS-Port-Type k) Service-Type l) User-Name m) parametrów sesji w tym:	
		i. typu żądania agenta na stacji końcowej (początkowe/initial lub reassessment) ii. architektury systemu operacyjnego na stacji końcowej (32-bit lub 64-bit) iii. adresu URL, z którego nastąpiło przekierowanie	
		System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, 10, Mac OS-X, pod kątem zainstalowanych aplikacji Antywirusowych (AV Compound Condition), w tym: a) stwierdzenia czy system AV jest obecny na stacji b) stwierdzenia czy definicje sygnatur AV są nie starsze niż zadana ilość dni od: i. daty ostatniego pliku definicji ii. aktualnego czasu systemowego	
		System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, Mac OS-X pod kątem zainstalowanych aplikacji AntiSpyware (AS Compound Condition), w tym: a) stwierdzenia czy system AS jest	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		obecny na stacji b) stwierdzenia czy definicje sygnatur AS są nie starsze niż zadana ilość dni od: i. daty ostatniego pliku definicji ii. aktualnego czasu systemowego	
6.	Obsługa serwerów certyfikatów CA.	System musi posiadać funkcję zintegrowanego centrum certyfikacji, Certificate Authority (CA) lub zapewniać współpracę z zewnętrznym centrum CA.	
		Funkcja CA musi umożliwiać wystawianie certyfikatów dla urządzeń, które uzyskują dostęp do sieci w procesie BYOD, dla realizacji bezpiecznego uwierzytelniania przy pomocy EAP-TLS.	
		System musi wspierać hierarchiczność CA dla rozproszonego wdrożenia w dużej skali. W sytuacji rozproszenia systemu na wiele serwerów, serwery nadrzędne oferują funkcję Root CA, zaś serwery przetwarzające wspierają funkcję Subordinate CA (SCEP RA) dla wystawiania certyfikatów.	
		Funkcja CA musi zapewniać przynajmniej następujące funkcjonalności: a) Certificate Issuance: sprawdzenie i podpisywanie Certificate Signing Request (CSR) dla stacji końcowych, które chcą uzyskać dostęp do sieci za pomocą bezpiecznej metody uwierzytelniania EAP-TLS b) Key Management: generacja i bezpieczne przechowywanie kluczy i certyfikatów w modelu rozproszonym c) Certificate Storage: bezpieczne przechowywanie certyfikatów użytkowników i stacji d) Online Certificate Status Protocol (OCSP): wsparcie dla sprawdzenia ważności certyfikatów za pomocą protokołu OCSP wraz ze wsparciem dla wysokiej dostępności, przynajmniej dwóch serwerów OCSP per CA	
7.	Raportowanie	System musi umożliwiać generowanie raportów dla protokołów AAA:	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		a) diagnostyki protokołów AAA b) trendów uwierzytelnienia 802.1X c) accountingu RADIUS d) uwierzytelniania RADIUS	
		System musi umożliwiać generowanie raportów dozwolonych protokołów a) sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym: i. uwierzytelnień pomyślnych ii. uwierzytelnień nieudanych iii. „N" największych ilości uwierzytelnień RADIUS per protokół EAP (Top5), w tym: uwierzytelnień pomyślnych i nieudanych	
		System musi umożliwiać generowanie raportów dla poszczególnych instancji serwerów systemu, w tym: a) uwierzytelnień RADIUS per serwer b) Top „N"uwierzytelnień per serwer c) monitorowania Online Certificate d) Status Protocol (OCSP) e) administratorów systemu i ich uprawnień f) logowania administratorów do systemu g) zmian konfiguracji serwera dokonanych przez administratorów h) stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS) i) zmian operacyjnych serwera dokonanych przez administratorów j) zmian haseł przez użytkowników	
		System musi umożliwiać generowanie raportów dla stacji końcowych, w tym: a) uwierzytelnień typu MAC Authentication b) Top „N"uwierzytelnień per adres MAC stacji c) Top „N" uwierzytelnień per maszyna d) Top „N"uwierzytelnień per RADIUS Calling Station ID e) działań podsystemu profilera per adres MAC f) czasu wymaganego na sprofilowanie stacji per adres MAC	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		System musi umożliwiać generowanie raportów dla błędów, w tym: a) błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił b) sumarycznych przyczyn nieudanych uwierzytelnień c) Top „N" uwierzytelnień per rodzaj błędu	
		System musi umożliwiać generowanie raportów dla urządzeń sieciowych: a) sumarycznych uwierzytelnień dla urządzeń sieciowych b) Top „N" uwierzytelnień per urządzenie sieciowe c) niedostępności serwera AAA dla urządzenia sieciowego d) wiadomości logowanych przez urządzenia sieciowe e) stanu portów i sesji urządzenia sieciowego widocznych przez SNMP	
		System musi umożliwiać generowanie raportów użytkowników: a) sumarycznych uwierzytelnień użytkowników b) Top „N"uwierzytelnień per użytkownik c) sesji użytkowników gościnnych d) aktywności użytkowników gościnnych e) sumarycznych uwierzytelnień sponsorów dostępu gościnnego f) uwierzytelnień per unikalny użytkownik	
		System musi umożliwiać generowanie raportów katalogu sesji a) aktywnych sesji RADIUS b) historii sesji RADIUS c) zaterminowanych sesji RADIUS	
8.	Alarmy	System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą: a) wiadomości e-mail b) syslog	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Alarmy muszą być generowane w następujących sytuacjach: a) ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu b) opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego c) status krytycznych procesów będzie niepożądany, w tym status: i. procesu wewnętrznej bazy danych systemu ii. serwera aplikacyjnego systemu iii. bazy danych sesji iv. kolektora i procesora wiadomości log v. błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej) vi. stan obciążenia systemu oraz zajętości pamięci wzrośnie powyżej zadanego poziomu	
		System musi posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym: a) badanie łączności IP za pomocą ping, nslookup, traceroute b) wyszukiwanie zdarzeń RADIUS z uwzględnieniem: i. nazwy użytkownika ii. adresu MAC iii. statusu uwierzytelnienia (udana lub nieudana) iv. powodu, jeżeli uwierzytelnienie nieudane v. zakresu czasowego, co do dnia, godziny i minuty c) wykonanie zdalnego polecenia na urządzeniu sieciowym d) ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem: i. definicji serwerów AAA ii. protokołu RADIUS iii. odkrywania urządzeń iv. logowania v. uwierzytelniania Web vi. konfiguracji trybu 802.1X	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		e) wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu	
9.	Dopuszczalne sposoby realizacji rozwiązania	Zamawiający wymaga spełnienia następujących warunków realizacji systemu uwierzytelnienia dostępu do sieci: a) Zamawiający dopuszcza stosowanie pojedynczego rozwiązania jak też systemu złożonego z kilku komponentów. b) W przypadku zastosowania rozwiązań złożonych z kilku komponentów różnych dostawców Zamawiający oczekuje, iż system będzie zapewniał pojedynczy interfejs konfiguracyjny, zarządzający i monitorujący zapewniający możliwość wymuszenia spójnej polityki bezpieczeństwa dla dostępu LAN. Zamawiający będzie traktował to rozwiązanie jako integralne części systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia) c) W przypadku zastosowania rozwiązań złożonych z kilku komponentów różnych dostawców	
		d) Zamawiający oczekuje iż system będzie serwisowany przez jednego producenta tzn. zgłoszenia serwisowe będą kierowane do jednego dostawcy. Zamawiający będzie traktował to rozwiązanie jako integralne części systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia). e) W przypadku zastosowania serwera CA jako dedykowanego rozwiązania Zamawiający będzie traktował to rozwiązanie jako integralną część systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia)	
	Licencje	Wykonawca dostarczy min. 4500 licencji bazowych do systemu uwierzytelnienia i profilowania użytkowników.	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		System musi być w pełni kompatybilny z urządzeniami dostarczonymi przez Wykonawcę.	

OŚWIADCZAMY, ŻE

1. **Jestem / nie jestem * Wykonawcą z sektora małych i średnich przedsiębiorstw.**
2. Pozostajemy związani niniejszą ofertą przez 30 dni licząc od dnia, w którym upłynął termin składania ofert.
3. Oświadczamy, że podane w niniejszej ofercie ceny za wykonanie przedmiotu zamówienia w czasie trwania umowy nie ulegną zmianie.
4. W cenie oferty zostały uwzględnione wszystkie koszty wykonania zamówienia i realizacji przyszłego świadczenia umownego.
5. Zawarty w Specyfikacji Istotnych Warunków Zamówienia wzór umowy został przez nas zaakceptowany i zobowiązujemy się w przypadku udzielenia nam zamówienia do zawarcia umowy w miejscu i terminie wyznaczonym przez Zamawiającego.
6. Wykonawca oświadcza, że posiada autoryzację producenta sprzętu oraz dysponuje własnym działem serwisu (wsparcia).
7. Wadium wniesione w pieniądzu należy zwrócić na poniższy rachunek bankowy:

   .....

8. Osobą upoważnioną do realizacji przedmiotu zamówienia jest: ....., tel. ....., e-mail: .....

.....dnia .....

.....
(podpis i pieczątka imienna przedstawiciela Wykonawcy/Pełnomocnika)

Podpisy i pieczątki imienne osób upełnomocnionych do reprezentowania Wykonawcy zgodnie z zapisami w dokumencie stwierdzającym status prawny.