

1. Zestaw komputerowy wraz z monitorem – 40 szt.

Zestaw komputerowy wraz z monitorem	
Podzespół	Minimalne parametry
Typ komputera	Komputer stacjonarny w formie Small Form Factor (SFF)
Procesor	<ol style="list-style-type: none"> 1. Procesor klasy x86, 64 bitowy, umożliwiający osiągnięcie przez oferowany zestaw komputerowy w teście SYSmark® 2018 wyniku całkowitego Overall Performance – min. 2100 punktów w oparciu o wyniki testów opublikowane na stronie konsorcjum BAPCo lub wyników testu przeprowadzonego przy pomocy oryginalnego oprogramowania testującego BAPCo zawierających wbudowane pliki FDR - tzw. Full DisclosureReports. 2. Wydajność zaoferowanego procesora minimum 19500 pkt.na podstawie informacji uzyskanych w teście PassMark CPU Performance. Test w kolumnie PassMark CPU Mark według wyników testów procesorów opublikowanych na stronie: http://www.cpubenchmark.net/cpu_list.php <p><u>Zamawiający zweryfikuje wydajność zaoferowanego procesora według wyników testów procesorów opublikowanych na stronie:</u> http://www.cpubenchmark.net/cpu_list.php</p>
Płyta główna	<ol style="list-style-type: none"> 1. minimum 1 x PCI Express x 16 2. minimum 1 x PCI Express x 1
Pamięć operacyjna RAM	<ol style="list-style-type: none"> 1. minimum 16GB DDR4 2. możliwość rozszerzenia do minimum 64GB DDR4 ,
Zewnętrzne łącza minimum	<ol style="list-style-type: none"> 1. minimum 2 porty cyfrowe (wymagane załączenie jednego przewodu łączącego monitor z komputerem z wykorzystaniem portów cyfrowych, nie dopuszcza się stosowania adapterów, przejściówek, kart rozszerzeń itp.), 2. minimum 1 port sieciowy RJ-45,

	<ol style="list-style-type: none"> 3. minimum 8 x USB, w tym: min. 4 porty min. USB 3.0 i min. 4 porty USB 2.0, 4. porty słuchawek i mikrofonu na przednim panelu obudowy. Zamawiający dopuszcza złącze typu combo.
Dysk twardy	Pojemność minimum 256GB SSD M2 w standardzie PCIe NVME.
Napęd optyczny	Nagrywarka DVD +/-RW typu slim z dołączonym oprogramowaniem do nagrywania i odtwarzania, dopuszcza się oprogramowanie zintegrowane z systemem operacyjnym
Wbudowane co najmniej	<ol style="list-style-type: none"> 1. Karta dźwiękowa 2. Karta sieciowa 10/100/1000 Ethernet, zintegrowana z płytą główną wspierająca obsługę technologii WoL oraz wspierającą łączność bezprzewodową obsługującą standard min. 802.11ac oraz łączność Bluetooth w wersji min. 5.0
Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Pełna obsługa funkcji i standardów DX12, OpenGL 4.5
BIOS	<p>Minimalna funkcjonalność:</p> <ol style="list-style-type: none"> 1. konfiguracja hasła użytkownika i administratora, 2. blokada portów USB
Klawiatura	Klawiatura USB w układzie polskim programisty (104 klawisze).
Mysz	Mysz optyczna USB z klawiszami oraz rolką (scroll).
Obudowa	<ol style="list-style-type: none"> 1. Obudowa typu Small Form Factor (SFF) z możliwością pracy w pozycji pionowej i poziomej,
Zasilacz	Zasilacz o sprawności min. 82%. Kabel zasilający.
Bezpieczeństwo i funkcje zarządzania	<ol style="list-style-type: none"> 1. Możliwość zastosowania mechanicznego zabezpieczenia przed kradzieżą komputera, 2. Możliwość zastosowania mechanicznego zabezpieczenia przed niepożądanym dostępem do wnętrza obudowy, 3. Moduł TPM 2.0.
Sterowniki	Zapewnienie na dedykowanej stronie internetowej producenta dostępu do najnowszych sterowników i uaktualnień, realizowane poprzez

	<p>podanie numeru seryjnego/modelu urządzenia, link strony www.</p> <p>Uwaga: w Formularzu cenowym należy wpisać link strony.</p>
Certyfikaty i oświadczenia	<ol style="list-style-type: none"> 1. Oferowane Komputery stacjonarne muszą posiadać europejską deklarację zgodności CE. 2. Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 10 w wersji Professional lub w przypadku zaoferowania komputerów z systemem równoważnym muszą posiadać certyfikat zgodności z zainstalowanym systemem operacyjnym.
Zainstalowane oprogramowanie	<p>Zainstalowany system operacyjny co najmniej Windows 10 Professional 64 bitowy w polskiej wersji językowej lub system równoważny.</p> <p>Klucz licencyjny systemu musi być zapisany trwale w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego.</p> <p><u>Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu.</u></p> <p>System równoważny musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:</p> <ol style="list-style-type: none"> 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ol style="list-style-type: none"> a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykaniem na urządzeniach typu tablet lub monitorach dotykowych. 2. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim. 3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimedialny, pomoc, komunikaty systemowe. 4. Wbudowany system pomocy w języku polskim. 5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.

	<ol style="list-style-type: none"> 6. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. 7. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. 8. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne. 9. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 10. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 11. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 12. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 13. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). 14. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. 15. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. 16. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>dla systemu operacyjnego i dla wskazanych aplikacji.</p> <ol style="list-style-type: none">17. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.18. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.19. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urzędnika na uprawniony dostęp do zasobów tego systemu.20. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.21. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.22. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).23. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.24. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.25. Mechanizmy logowania do domeny w oparciu o:<ol style="list-style-type: none">a. Login i hasło,b. Karty z certyfikatami (smartcard),c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).26. Mechanizmy wieloelementowego uwierzytelniania.27. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5.
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>28. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.</p> <p>29. Wsparcie dla algorytmów Suite B (RFC 4869).</p> <p>30. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.</p> <p>31. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.</p> <p>32. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p> <p>33. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.</p> <p>34. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,</p> <p>35. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.</p> <p>36. Rozwiązanie ma umożliwiający wdrożenie nowego obrazu poprzez zdalną instalację.</p> <p>37. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.</p> <p>38. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.</p> <p>39. Udostępnianie modemu.</p> <p>40. Oprogramowanie dla tworzenia kopii zapasowych (Backup);</p>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.</p> <p>41. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.</p> <p>42. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).</p> <p>43. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).</p> <p>44. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.</p> <p>45. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.</p> <p>46. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.</p> <p>47. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.</p> <p>48. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.</p> <p>49. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	konieczności reinstalacji systemu.
Gwarancja	<p>Gwarancja jakości producenta:</p> <ol style="list-style-type: none"> 1. Na okres co najmniej 36 miesięcy w systemie Door to Door lub w lokalizacji Zamawiającego, jeżeli naprawa wymaga wykonania jej w miejscu instalacji. Koszt transportu do i z naprawy pokrywa Wykonawca. 2. Czas reakcji na zgłoszoną reklamację gwarancyjną do końca następnego dnia roboczego. 3. Czas naprawy od momentu zgłoszenia do 14 dni roboczych. 4. Naprawy gwarancyjne urządzeń muszą być realizowane przez serwis producenta lub Autoryzowanego Partnera Serwisowego Producenta. 5. W przypadku awarii dysków twardech dysk pozostaje u Zamawiającego. 6. W przypadku gdy firma serwisująca jest inna niż producent komputerów to musi posiadać autoryzację producenta komputera – oświadczenie zawarte w Formularzu ofertowym 7. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
	Monitor
Przekątna ekranu	Min. 27"
Typ matrycy	VA lub IPS
Jasność	Min. 250 cd/m ²
Kontrast statyczny:	Min. 1000:1
Częstotliwość odświeżania	Min. 60Hz
Czas reakcji matrycy	Maks. 5ms
Rozdzielczość wyświetlania	Min. 1920 x 1080
Zakres pochylenia	Min. od 20° w górę do 5° w dół

monitora	
Złącze	Min: złącze cyfrowe HDMI oraz złącze VGA
Głośniki	Wbudowane głośniki lub dedykowana przez producenta listwa głośnikowa.
Inne:	<ol style="list-style-type: none"> 1) Monitor musi posiadać możliwość zainstalowania na ścianie przy wykorzystaniu ściennego systemu montażowego VESA. 2) Monitor musi posiadać komplet kabli, w tym odpowiedni do złącza kabel do sygnału cyfrowego tożsamy z portem video zastosowanym w komputerze, kabel audio do przesyłania dźwięku do głośników wbudowanych w monitorze, kabel zasilający. W przypadku zaoferowania monitora wyposażonego w dedykowaną przez producenta listwę głośnikową, Wykonawca nie ma obowiązku dostarczenia kabla audio do przesyłania dźwięku do głośników wbudowanych w monitorze natomiast Zamawiający wymaga dostarczenia kabla umożliwiającego podłączenie zaoferowanej listwy głośnikowej do zaoferowanego modelu monitora.
Gwarancja	<p>Gwarancja jakości producenta:</p> <ol style="list-style-type: none"> 1. Na okres co najmniej 36 miesięcy w systemie Door to Door. Koszt transportu do i z naprawy pokrywa Wykonawca. 2. Czas reakcji na zgłoszoną reklamację gwarancyjną do końca następnego dnia roboczego. 3. Czas naprawy od momentu zgłoszenia do 14 dni roboczych.

2. UTM typ 1 – lokalizacja główna – 1 szt.

UTM Typ 1 – lokalizacja główna	
Architektura systemu	
<ol style="list-style-type: none"> 1. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, umożliwiającej rozbudowę do dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności conajmniej Active-Passive, o specyfikacji opisanej poniżej 2. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. 3. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent. 	
<ol style="list-style-type: none"> 1. Metalowa obudowa o wysokości max. 1U przeznaczona do montażu w szafie RACK 19'' 2. Obsługa nielimitowanej ilości hostów w sieci chronionej. 3. Minimalna liczba i typ interfejsów fizycznych: <ul style="list-style-type: none"> •System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000 •System realizujący funkcję Firewall musi dysponować minimum 2 interfejsami optycznymi 10GbE (SFP+) •System realizujący funkcję Firewall musi umożliwiać wymianę dostępnych interfejsów na minimum 4 interfejsy optyczne 10GbE (SFP+) •Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q. 4. Minimalna liczba nowych połączeń na sekundę: 40 000 5. Minimalna liczba jednoczesnych połączeń: 1 000 000 6. Minimalna przepustowość Firewall: 15 Gbps 7. Minimalna przepustowość IPS: 8 Gbps 8. Minimalna przepustowość Threat Protection: 2 Gbps 9. Minimalna przepustowość IPSec VPN: 3 Gbps 10. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 200 GB SSD do celów logowania i raportowania 	
PODSTAWOWE FUNKCJE SYSTEMU OCHRONY	
Zarządzanie i utrzymanie	<ol style="list-style-type: none"> 1. Rozwiązanie musi być zarządzane przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu

	<p>konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH.</p> <ol style="list-style-type: none"> 2. Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej ping 3. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 4. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 5. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. 6. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego 7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników. 8. Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora. 9. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP 10. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3 11. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do chmury producenta lub własnego serwera. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, tygodniowo oraz miesięcznie. 12. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware)
<p>Zapora sieciowa, konfiguracja sieciowa oraz routing</p>	<ol style="list-style-type: none"> 1. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection. 2. Rozwiązanie musi umożliwiać budowanie reguł zapory sieciowych w oparciu o takie obiekty jak elementy jak host, sieć, interfejs, harmonogram, port, protokół, użytkownik, grupa użytkowników, metoda uwierzytelnienia 3. System musi umożliwiać budowanie reguł bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane

	<p>przez administratora harmonogramy czasowe.</p> <ol style="list-style-type: none"> 4. Rozwiązanie musi pozwolić na definiowanie własnych polityk NAT wraz z IP masquerading. 5. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection). 6. System musi zapewniać ochronę przed skanowaniem portów (portscan blocking). 7. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). 8. Rozwiązanie musi zapewniać obsługę routingu statycznego. 9. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, OSPF, BGP). 10. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z obsługą RSTP oraz MSTP. 11. System musi oferować funkcjonalność serwera DHCP lub DHCP Relay. 12. System musi oferować wsparcie dla IEEE 802.1Q VLAN z niezależnymi pulami DHCP. 13. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. 14. Rozwiązanie musi umożliwiać rozkładanie ruchu do Internetu w oparciu o wagi poszczególnych bram ISP. 15. Wymagane jest by rozwiązanie zapewniało obsługę modemu USB LTE np. jako łącze zapasowe . 16. Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). 17. Rozwiązanie musi dawać możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza. 18. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 19. Rozwiązanie musi dawać możliwość optymalizacji ruchu wychodzącego w dostępie do określonych usług. 20. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. 21. System musi dawać możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.
<p>Podstawowe kształtowanie pasma</p>	<ol style="list-style-type: none"> 1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla użytkownika, hosta lub połączenia.

oraz limity ilości danych	<ol style="list-style-type: none"> 2. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
Autoryzacja użytkowników	<ol style="list-style-type: none"> 1. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont. 2. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP 3. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory 4. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP. 5. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal. 6. Rozwiązanie musi posiadać wbudowany moduł zapewniający uwierzytelnianie na poziomie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 7. Metoda 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
Samoobsługowy portal dla użytkowników	<ol style="list-style-type: none"> 1. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). 2. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta OpenVPN dla Windows, Mac OS X, Linux, iOS, Android 3. Rozwiązanie musi umożliwiać zmianę hasła.
Podstawowe opcje VPN	<p>System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:</p> <ol style="list-style-type: none"> 1. Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK) 2. Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
OCHRONA SIECI	
IPS	<ol style="list-style-type: none"> 1. Dodatkowy moduł ochrony klasy IPS z bazą minimum 1000 sygnatur. 2. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS. 3. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń. 4. Rozwiązanie musi oferować możliwość wyłączenia/włączenia

	<p>poszczególnych kategorii/sygnatur</p> <p>5. System musi generować alerty w przypadku wykrycia ataku.</p>
<p>OCHRONA I KONTROLA WEB ORAZ APLIKACJI</p>	
<p>Ochrona i kontrola Web</p>	<ol style="list-style-type: none"> 1. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS. 2. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP. 3. Rozwiązanie musi zapewniać skanowanie AV plików w czasie rzeczywistym 4. Rozwiązanie musi oferować funkcję inspekcji z obsługą protokołu TLS 1.3 oraz z tzw. walidacją certyfikatów. 5. System musi filtrować pliki na podstawie MIME. 6. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch. 7. Rozwiązanie musi zawierać przynajmniej 50 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www. 8. Rozwiązanie musi zapewniać możliwość blokowanie i wysyłania treści poprzez HTTP i HTTPS. 9. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego.
<p>Ochrona i kontrola aplikacji</p>	<ol style="list-style-type: none"> 1. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji. 2. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook) 3. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
<p>Kształtowanie pasma dla Web i Aplikacji</p>	<ol style="list-style-type: none"> 1. Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download. 2. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu. 3. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym.
<p>OCHRONA ANTYWIRUSOWA</p>	

<p style="text-align: center;">Ochrona i kontrola Email</p>	<ol style="list-style-type: none"> 1. Rozwiązanie musi oferować możliwość trybu pracy Transparent Email Proxy 2. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S. 3. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP. 4. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń. 5. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników. 6. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL. 7. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów email. 8. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka.
<p>OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY</p>	
<p style="text-align: center;">On-cloud Sandboxing</p>	<p>Rozwiązaniem musi dawać możliwość rozbudowy o dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności:</p> <ol style="list-style-type: none"> 1. Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych np., .exe 2. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf. 3. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf. 4. Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym zip, arj, lha, rar, cab 5. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows .
<p>LOGOWANIE I RAPORTOWANIE</p>	
	<ol style="list-style-type: none"> 1. System musi umożliwiać składowanie oraz archiwizację logów. 2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. 3. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.

	<ol style="list-style-type: none"> 4. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych). 5. Rozwiązanie musi generować raporty w HTML i CSV. 6. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog. 7. System musi zapewniać podgląd wykorzystania łącza internetowego. 8. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP 9. Rozwiązanie musi oferować możliwość zanonimizowania danych.
POZOSTAŁE	
Certyfikaty	<p>Urządzenie musi posiadać:</p> <ul style="list-style-type: none"> - certyfikat Common Criteria; - certyfikat ICSA Labs dla funkcji VPN IPsec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE;
GWARANCJA I SERWIS	
Wymagania ogólne dla dostarczanych rozwiązań	<ul style="list-style-type: none"> • Dostarczone urządzenia muszą być fabrycznie nowe, nieużywane w innych projektach, nie wycofane z produkcji i pochodzić z legalnego, polskiego kanału dystrybucji. • Całość dostarczanego sprzętu musi pochodzić z autoryzowanego kanału sprzedaży producentów na teren Polski – ze względów gwarancyjnych niedopuszczalne jest dostarczanie sprzętu z tzw. brokerki, • Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie zapisanym w specyfikacjach sprzętu, • Całość dostarczonego sprzętu i oprogramowanie musi być ze sobą kompatybilna i pochodzić od jednego producenta, • Wykonawca winien w momencie dostawy przedłożyć dokumenty potwierdzające, że posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.
Warunki gwarancji i serwisu	<ul style="list-style-type: none"> • Na dostarczany sprzęt musi być udzielona min. 36-miesięczna gwarancja; Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była wymiana urządzeń zgodnie z metodyką i zaleceniami producenta dostarczonych rozwiązań, • Wykonawca lub autoryzowany serwis ma obowiązek przyjmowania zgłoszeń serwisowych w języku polskim przez telefon (od poniedziałku do piątku, w godzinach 8-17), e-mail lub WWW (przez całą dobę),

Wymagania dodatkowe	<p>Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiającą:</p> <ul style="list-style-type: none">• bezpłatne pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres trwania gwarancji i licencji• dostęp do dokumentacji sprzętu i oprogramowania,• dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,• dostęp do pomocy technicznej producenta. <p>Zamawiający w momencie odbioru otrzyma:</p> <ul style="list-style-type: none">• licencje obejmujące wszystkie wymagane moduły na okres min. 60 miesięcy• możliwość automatycznego pobierania subskrypcji dla wszystkich wymaganych modułów w okresie trwania licencji.
----------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3. UTM typ 2 – lokalizacje zdalne – 2 szt.

UTM typ 2 – lokalizacje zdalne	
ARCHITEKTURA SYSTEMU	
<ol style="list-style-type: none"> 1. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, umożliwiającą rozbudowę do dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności co najmniej Active-Passive, o specyfikacji opisanej poniżej 2. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. 3. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent. 	
<ol style="list-style-type: none"> 1. Metalowa obudowa typu desktop. 2. Obsługa nielimitowanej ilości hostów w sieci chronionej. 3. Minimalna liczba i typ interfejsów fizycznych: <ul style="list-style-type: none"> • System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000 • Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q. 4. Minimalna liczba nowych połączeń na sekundę: 18 000 5. Minimalna liczba jednoczesnych połączeń: 300 000 6. Minimalna przepustowość Firewall: 4 Gbps 7. Minimalna przepustowość IPS: 2,4 Gbps 8. Minimalna przepustowość Threat Protection: 495 Mbps 9. Minimalna przepustowość IPSec VPN: 600 Mbps 10. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 200 GB SSD do celów logowania i raportowania lub musi istnieć możliwość wykorzystania karty SD do celów logowania i raportowania. 	
PODSTAWOWE FUNKCJE SYSTEMU OCHRONY	
Zarządzanie i utrzymanie	<ol style="list-style-type: none"> 1. Rozwiązanie musi być zarządzane przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH. 2. Wbudowany webowy graficzny interfejs użytkownika musi oferować

	<p>narzędzia diagnostyczne, co najmniej ping</p> <ol style="list-style-type: none"> 3. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 4. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 5. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. 6. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego 7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników. 8. Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora. 9. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP 10. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3 11. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do chmury producenta lub własnego serwera. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, tygodniowo oraz miesięcznie. 12. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware)
<p style="text-align: center;">Zapora sieciowa, konfiguracja sieciowa oraz routing</p>	<ol style="list-style-type: none"> 1. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection. 2. Rozwiązanie musi umożliwiać budowanie reguł zapory sieciowych w oparciu o takie obiekty jak elementy jak host, sieć, interfejs, harmonogram, port, protokół, użytkownik, grupa użytkowników, metoda uwierzytelnienia 3. System musi umożliwiać budowanie reguł bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. 4. Rozwiązanie musi pozwolić na definiowanie własnych polityk NAT wraz z IP masquerading. 5. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection). 6. System musi zapewniać ochronę przed skanowaniem portów (portscan

	<p>blocking).</p> <ol style="list-style-type: none"> 7. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). 8. Rozwiązanie musi zapewniać obsługę routingu statycznego. 9. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, OSPF, BGP). 10. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z obsługą RSTP oraz MSTP. 11. System musi oferować funkcjonalność serwera DHCP lub DHCP Relay. 12. System musi oferować wsparcie dla IEEE 802.1Q VLAN z niezależnymi pulami DHCP. 13. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. 14. Rozwiązanie musi umożliwiać rozkładanie ruchu do Internetu w oparciu o wagi poszczególnych bram ISP. 15. Wymagane jest by rozwiązanie zapewniało obsługę modemu USB LTE np. jako łącze zapasowe . 16. Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). 17. Rozwiązanie musi dawać możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza. 18. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 19. Rozwiązanie musi dawać możliwość optymalizacji ruchu wychodzącego w dostępie do określonych usług. 20. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. 21. System musi dawać możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.
<p>Podstawowe kształtowanie pasma oraz limity ilości danych</p>	<ol style="list-style-type: none"> 1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla użytkownika, hosta lub połączenia. 2. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
<p>Autoryzacja użytkowników</p>	<ol style="list-style-type: none"> 1. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 100 kont. 2. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP 3. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i

	<p>identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory</p> <ol style="list-style-type: none"> Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal. Rozwiązanie musi posiadać wbudowany moduł zapewniający uwierzytelnianie na poziomie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). Metoda 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
Samoobsługowy portal dla użytkowników	<ol style="list-style-type: none"> Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). Rozwiązanie musi udostępniać plik z konfiguracją dla klienta OpenVPN dla Windows, Mac OS X, Linux, iOS, Android Rozwiązanie musi umożliwiać zmianę hasła.
Podstawowe opcje VPN	<p>System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:</p> <ol style="list-style-type: none"> Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK) Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
OCHRONA SIECI	
IPS	<ol style="list-style-type: none"> Dodatkowy moduł ochrony klasy IPS z bazą minimum 1000 sygnatur. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń. Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur System musi generować alerty w przypadku wykrycia ataku.
OCHRONA I KONTROLA WEB ORAZ APLIKACJI	
Ochrona i kontrola Web	<ol style="list-style-type: none"> Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.

	<ol style="list-style-type: none"> 3. Rozwiązanie musi zapewniać skanowanie AV plików w czasie rzeczywistym 4. Rozwiązanie musi oferować funkcję inspekcji z obsługą protokołu TLS 1.3 oraz z tzw. walidacją certyfikatów. 5. System musi filtrować pliki na podstawie MIME. 6. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch. 7. Rozwiązanie musi zawierać przynajmniej 50 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www. 8. Rozwiązanie musi zapewniać możliwość blokowanie i wysyłania treści poprzez HTTP i HTTPS. 9. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego.
Ochrona i kontrola aplikacji	<ol style="list-style-type: none"> 1. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji. 2. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook) 3. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
Kształtowanie pasma dla Web i Aplikacji	<ol style="list-style-type: none"> 1. Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download. 2. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu. 3. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym.
OCHRONA ANTYWIRUSOWA	
Ochrona i kontrola Email	<ol style="list-style-type: none"> 1. Rozwiązanie musi oferować możliwość trybu pracy Transparent Email Proxy 2. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S. 3. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP. 4. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń. 5. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników. 6. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL.

	<ol style="list-style-type: none"> 7. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów email. 8. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka.
OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY	
On-cloud Sandboxing	<p>Rozwiązaniem musi dawać możliwość rozbudowy o dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności:</p> <ol style="list-style-type: none"> 1. Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych np., .exe 2. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf. 3. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf. 4. Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym zip, arj, lha, rar, cab 5. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows .
LOGOWANIE I RAPORTOWANIE	
	<ol style="list-style-type: none"> 1. System musi umożliwiać składowanie oraz archiwizację logów. 2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. 3. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących. 4. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych). 5. Rozwiązanie musi generować raporty w HTML i CSV. 6. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog. 7. System musi zapewniać podgląd wykorzystania łącza internetowego. 8. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP 9. Rozwiązanie musi oferować możliwość zanonimizowania danych.
POZOSTAŁE	

<p>Certyfikaty</p>	<p>Urządzenie musi posiadać:</p> <ol style="list-style-type: none"> 1. certyfikat Common Criteria; 2. certyfikat ICSA Labs dla funkcji VPN IPsec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE;
<p>GWARANCJA I SERWIS</p>	
<p>Wymagania ogólne dla dostarczanych rozwiązań :</p>	<ol style="list-style-type: none"> 1. Dostarczone urządzenia muszą być fabrycznie nowe, nieużywane w innych projektach, nie wycofane z produkcji i pochodzić z legalnego, polskiego kanału dystrybucji. 2. Całość dostarczanego sprzętu musi pochodzić z autoryzowanego kanału sprzedaży producentów na teren Polski – ze względów gwarancyjnych niedopuszczalne jest dostarczanie sprzętu z tzw. brokerki, 3. Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie zapisanym w specyfikacjach sprzętu, 4. Całość dostarczonego sprzętu i oprogramowanie musi być ze sobą kompatybilna i pochodzić od jednego producenta, 5. Wykonawca winien w momencie dostawy przedłożyć dokumenty potwierdzające, że posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.
<p>Warunki gwarancji i serwisu :</p>	<ol style="list-style-type: none"> 1. Na dostarczany sprzęt musi być udzielona min. 36-miesięczna gwarancja; Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była wymiana urządzeń zgodnie z metodyką i zaleceniami producenta dostarczonych rozwiązań, 2. Wykonawca lub autoryzowany serwis ma obowiązek przyjmowania zgłoszeń serwisowych w języku polskim przez telefon (od poniedziałku do piątku, w godzinach 8-17), e-mail lub WWW (przez całą dobę),
<p>Dodatkowe wymagania</p>	<p>Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiającą:</p> <ol style="list-style-type: none"> 1. bezpłatne pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres trwania gwarancji i licencji 2. dostęp do dokumentacji sprzętu i oprogramowania, 3. dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej, 4. dostęp do pomocy technicznej producenta. <p>Zamawiający w momencie odbioru otrzyma:</p> <ol style="list-style-type: none"> 1. licencje obejmujące wszystkie wymagane moduły na okres min. 60 miesięcy 2. możliwość automatycznego pobierania subskrypcji dla wszystkich wymaganych modułów w okresie trwania licencji.

4. Switch – 7 szt.

Switch	
NAZWA KOMPONENTU	WYMAGANE MINIMALNE PARAMETRY TECHNICZNE
Typ i liczba portów	Min. 48x portów 10/100/1000 Mbps RJ45 Min. 4x porty Gigabit SFP
Konsola	Port konsoli
Przepustowość	Min. 77 Mpps
Wydajność	Min. 104 Gbps
Tablica MAC	Tablica adresów MAC o wielkości minimum 8 000 pozycji.
Ramki Jumbo	Obsługa ramek Jumbo o wielkości minimum 9 KB
Funkcje	<p>Przełącznik zarządzany musi posiadać następujące funkcjonalności:</p> <ul style="list-style-type: none"> • Obsługa Quality of Service. • Obsługa mechanizmów: strict priority (SP) queuing, weighted round robin (WRR) oraz SP+WRR • Obsługa SpanningTree / STP • Obsługa sieci IEEE 802.1Q VLAN • Obsługa IGMP Snooping v1/v2/v3, MLD snooping v1/v2 • Obsługa statycznego routingu • Serwer DHCP, klient DHCP, DHCP snooping • Obsługa list ACL • Obsługa kontroli przepustowości • Obsługa izolacji portów • Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia • Obsługa standardu 802.1p • Możliwość zmiany wartości pola DSCP i/lub wartości priorytetu 802.1p • Funkcje mirroringu portów: RMON • Obsługa funkcji logowania do sieci („Network Login”) zgodna ze standardem IEEE 802.1x • Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS oraz wsparcie dla TACACS/TACACS+. • Zarządzanie poprzez port konsoli • Syslog • Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) oraz LLDP-MED • Obsługa Simple Network Time Protocol (SNTP)
Obudowa	<ul style="list-style-type: none"> • Wysokość w szafie 19” – 1U
Wymagania dodatkowe	<ul style="list-style-type: none"> • Wszystkie przełączniki powinny pochodzić z oficjalnego kanału dystrybucji

	producenta. <ul style="list-style-type: none"> • Wszystkie przełączniki muszą być fabrycznie nowe.
Gwarancja	<ul style="list-style-type: none"> • Gwarancja min. 36 miesięcy

5. Szafa ogniotrwała – 1 szt.

Szafa ogniotrwała	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Pojemność	Min. 32 L
Wymiary zewnętrzne	Szafa ogniotrwała musi mieć wymiary: <ul style="list-style-type: none"> • Wysokość min. 450 mm • Szerokość min. 450 mm • Głębokość minimum 450 mm.
Odporność na ogień	Szafa musi chronić przed ogniem przez min. 60 min
Certyfikaty	Szafa ogniotrwała musi posiadać następujące certyfikaty: <ul style="list-style-type: none"> • EN 15659 • EN 14450