Załącznik nr 5 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Wszystkie dostarczone urządzenia mają być skonfigurowane zgodnie z zaleceniami Zamawiającego. Sprzęt ma zostać dostarczony do siedziby Zamawiającego.

1.UTM – 1 szt.
Minimalne wymagania oferowanego sprzętu:

Lp.	Parametry	Wymagania minimalne
1.	System – konstrukcja	Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca) Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie HA Active-Passive lub Active-Active. Rozwiązanie powinno być wyposażone w wysokowydajny wielordzeniowy procesor x86 (CPU) oraz dodatkowo w procesor (NPU) do akceleracji ruchu dla warstwy aplikacji. Rozwiązanie musi być wyposażone w co najmniej jeden dysk SSD służący m.in. do przechowywania logów i raportów bezpośrednio na urządzeniu. Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy (drugi zasilacz jako wyposażenie opcjonalne). Urządzenie w metalowej obudowie o wysokości 1U z możliwością montażu w szafie Rack 19" (uchwyty montażowe w komplecie). Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB). Wbudowany port Ethernet do zarządzania w trybie out-of-band management. Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie. Wbudowany port USB umożliwiający podłączenie pamięci flash i przeprowadzenie konfiguracji w trybie Zero Touch. Możliwość rozbudowy o dodatkowe moduły interfejsów sieciowch. Zintegrowany wielofunkcyjny wyświetlacz LCD informujący o stanie pracy urządzenia.
2.	Pamięć operacyjna RAM	nie mniej niż 8 GB
3.	Przestrzeń do przechowywania logów i raportów	nie mniej niż 120 GB

4.	Liczba fizycznych interfejsów 1000BASE-T	nie mniej niż 8
5.	Liczba fizycznych interfejsów 1000BASE-X	nie mniej niż 2
6.	Liczba fizycznych interfejsów 10GBASE-X	nie mniej niż: -
7.	Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q	nie mniej niż 128
8.	Wydajność Firewall	nie mniej niż 30 Gbps
9.	Wydajność Firewall IMIX	nie mniej niż 15 Gbps
10.	Wydajność IPS	nie mniej niż 5,8 Gbps
11.	Wydajność FW+IPS+AV	nie mniej niż 1,25 Gbps
12.	Wydajność NGFW	nie mniej niż 5,2 Gbps
13.	Liczba równoczesnych połączeń	nie mniejsza niż 6500000
14.	Liczba nowych połączeń na sekundę	nie mniejsza niż 134700
15.	Wydajność IPsec VPN	nie mniej niż 12 Gbps
16.	Wydajność dla inspekcji ruchu SSL/TLS	nie mniej niż 1,1 Gbps
17.	Liczba równoczesnych połączeń SSL/TLS	nie mniejsza niż 18432
18.	Liczba równoczesnych tuneli SSL VPN	nie mniejsza niż 2500
19.	Liczba równoczesnych tuneli IPsec VPN	nie mniejsza niż 2600
20.	Zarządzanie	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN.

		Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter. Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. Rozwiązanie powinno oferować wiersz poleceń dostępny z poziomu graficznego interfejsu administratora, portu konsolowego oraz za pośrednictwem protokołu SSH z uwierzytelnianiem przy użyciu kluczy RSA, DSA lub ECDSA o długości min. 2048 bitów. Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog). Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej. System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS). Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i

		aktualizowane przez producenta. System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpowiednika). System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia. System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta, przy czym w podstawowej wersji utrzymywany i udostępniany jest on bezpłatnie i nie wymaga zakupu osobnych subskrypcji. Wymagane jest, aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP, via email jak i dodatkowo do centralnego systemu zarządzania w chmurze. Rozwiązanie powinno oferować wbudowany mechanizm pozwalający na automatyczne tworzenie szyfrowanych hasłem kopii zapasowych konfiguracji w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu. Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich. Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej. Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu licencyjnego a synchronizacja subskrypcji powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). Informacja o dostępności nowej wersji powinna pojawiać się w Web GUI. Producent powinien oferować mechanizm automatycznego łatania wykrytych w oprogramowaniu systemowym podatności przez tzw. hotfixies, przy czym administrator powinien móc funkcjonalność tą wyłączyć. Rozwiązanie powinno oferować mechanizm szyfrowania danych takich jak loginy, hasła, klucze które przechowywane są w konfiguracji urządzenia. Dane powinny być zabezpieczone dedykowanym kluczem szyfrującym tworzonym na podstawie bezpiecznie składowanego poza urządzeniem hasła. Rozwiązanie powinno zapewniać możliwość zmiany nazw interfejsów sieciowych.
21.	Zapora sieciowa	Wymagane jest, aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection. System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6. Rozwiązanie

		powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas. System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. System powinien pozwalać na selektywne wyłączanie reguł zapory sieciowej (bez konieczności ich usuwania). System powinien pozwalać na grupowanie reguł zapory. Wymagana jest funkcjonalność automatycznego wiązania nowotworzonych reguł do właściwych grup na podstawie kryteriów opisujących grupę. Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. System ochrony powinien zawierać predefiniowane strefy zapory typu: LAN, WAN, DMZ, VPN. Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej. System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). Rozwiązanie powinno oferować narzędzie do symulowanego testu reguł zapory w oparciu o zadane przez administratora kryteria takie jak IP, strefa zapory, użytkownik, dzień, godzina. System powinien pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika.
22.	Trasowanie ruchu	Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing. Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów. Rozwiązanie powinno umożliwiać rozkładanie ruchu w oparciu o wagi interfejsów WAN. Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast. Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM). Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6.

23.	Translacja adresów i portów	Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT. Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT. Rozwiązanie powinno pozwalać na automatyczne tworzenie reguł NAT typu loopback czy reflexive rule.
24.	Kształtowanie pasma i jakość usług	System powinien zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji. Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne. System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6. Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet (od 1 Business Critical do 7 Best Effort).
25.	Podstawowa ochrona przed atakami DoS i DDoS	System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
26.	Pozostałe	Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge). System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. System powinien oferować wsparcie dla IEEE 802.1Q VLAN z możliwością konfiguracji niezależnych puli DHCP. Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). System powinien oferować wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp. Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd). Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo). Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych.

27.	Kontroler sieci bezprzewodowej	System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania. Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Access Point, Wireless Bridge oraz Wireless Repeater. Uruchomienie punktów dostępowych sieci bezprzewodowej powinno odbywać się na zasadzie plug-and-play, gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu. Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej. Rozgłaszane sieci bezprzewodowe powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując przy tym możliwość izolacji klientów sieci bezprzewodowej. Rozwiązanie powinno umożliwiać rozgłaszanie wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej (Hide SSID). Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise. Rozwiązanie powinno zapewniać wsparcie dla uwierzytelniania klientów w oparciu o IEEE 802.1X (RADIUS Authentication). Rozwiązanie powinno oferować wsparcie dla IEEE 802.11r (Fast Transition). System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów. Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości. System powinien zapewniać możliwość tworzenia odseparowanej sieci dla gości w wariancie walled garden. System powinien pozwalać na rozgłaszanie sieci bezprzedowodych w oparciu o harmonogramy czasowe. Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych (Rogue AP detection).
28.	Uwierzytelnianie i obsługa użytkowników	Wymagane uwierzytelniaine użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta. Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników. System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+.

		Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory. System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm). Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server. System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu.
29.	Koncentrator VPN	System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2. System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519). System musi obsługiwać połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN. Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN. Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback. Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego. Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth. Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN.

		Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN. Urządzenie musi obsługiwać połączenia L2TP over IPsec. Połączenia VPN terminowane muszą być dedykowanej strefie zapory sieciowej.
30.	Logowanie i raportowanie	System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym. System powinien umożliwiać składowanie oraz archiwizację logów. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali. System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących. Rozwiązanie powinno umożliwiać wysyłanie raportów via email. Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV. Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog. System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza. System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację. Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach. System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.
31.	Intrusion Prevention System i Advanced Threat Protection	Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur. Wymagane jest, aby system automatycznie aktualizował sygnatury zagrożeń. Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS. Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS.

		System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet.
32.	Ochrona i kontrola web - Ochrona przez Malware	Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP. Rozwiązanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania. Dodatkowo rozwiązanie powinno umożliwiać uruchomienie silnika antywirusowego firmy trzeciej. Wymagane jest, aby system automatycznie aktualizował sygnatury zagrożeń. System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek. Rozwiązanie musi przeprowadzać emulację skryptów Java. Rozwiązanie powinno przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta. Rozwiązanie powinno umożliwiać blokowanie potencjalnie niechcianych aplikacji (tzw. Potentially Unwanted Applications - PUAs) System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates)
33.	Inspecja ruchu SSL/TLS	Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów. Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2. Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP. Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443). Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web. Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen.
34.	Filtr Web	Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron Web oraz umożliwiać dodawanie własnych kategorii stron. Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy.

		Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól. System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowania treści komunikatu w tym dodania logo organizacji. Rozwiązanie powinno umożliwiać filtrowanie stron web analizując ich zawartość wykorzystując tzw. Content Filtering na bazie haseł kluczowych. Rozwiązanie powinno oferować ochronę przed Pharmingiem.
35.	Ochrona i kontrola aplikacji	Rozwiązanie powinno oferować bazę danych opisująca co najmniej 3000 aplikacji. Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji. Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji. Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów. Rozwiązanie powinno umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp. Rozwiązanie powinno oferować funkcje CASB (Cloud Access Security Broker) celem monitorowania i regulowania dostępu do aplikacji chmurowych wykorzystywanych przez użytkowników. Rozwiązanie powinno umożliwiać tworzenie własnych grup aplikacji co najmniej na potrzeby polityk SD-WAN.
36.	Ochrona przed nieznanymi zagrożeniami	Rozwiązanie klasy Sandbox do ochrony przez zagrożeniami typu Zero-Day. Rozwiązanie oferujące statyczną i dynamiczną analizę kodu przesyłanego w ramach ruchu web czy email. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf. Rozwiązanie umożliwiające dodatkową inspekcję i detonację archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab. System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS. System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu. System zapewniający analizę struktury kodu w tym analizę przeprowadzaną przez mechanizmy głębokiego uczenia maszynowego.

		System zapewniający ochronę przed exploitami i złośliwym kodem ransomware. System badający reputację pliku w zewnętrznych bazach takich jak np.Virustotal. System powinien oferować szczegółowe raporty dowodzące przeprowadzanie analizy dla w/w mechanizmów.

2.UTM – 17 szt.
Minimalne wymagania oferowanego sprzętu:

Lp.	Parametry	Wymagania minimalne
1.	System – konstrukcja	System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania. Rozwiązanie powinno być wyposażone w moduł kryptograficzny zgodny ze standardem FIPS 140-2. Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca) Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie HA Active-Passive lub Active-Active. System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej. Rozwiązanie powinno być wyposażone w wysokowydajny wielordzeniowy procesor x86 (CPU) oraz dodatkowo w procesor (NPU) do akceleracji ruchu dla warstwy aplikacji. Rozwiązanie musi być wyposażone w co najmniej jeden dysk SSD służący m.in. do przechowywania logów i raportów bezpośrednio na urządzeniu. Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy (drugi zasilacz jako wyposażenie opcjonalne). Urządzenie w metalowej obudowie o wysokości 1U z możliwością montażu w szafie Rack 19" (uchwyty montażowe jako opcjonalne wyposażenie, w przypadku braku uchwytów montażowych należy dostarczyć półkę RACK na urządzenie). Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB). Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie.

		Wbudowany port USB umożliwiający podłączenie pamięci flash i przeprowadzenie konfiguracji w trybie Zero Touch. Możliwość rozbudowy o dodatkowe moduły interfejsów sieciowch.
2.	Pamięć operacyjna RAM	nie mniej niż 4 GB
3.	Przestrzeń do przechowywania logów i raportów	nie mniej niż 64 GB
4.	Liczba fizycznych interfejsów 1000BASE-T	nie mniej niż 8
5.	Liczba fizycznych interfejsów 1000BASE-X	nie mniej niż 1
6.	Liczba fizycznych interfejsów 10GBASE-X	nie mniej niż: -
7.	Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q	nie mniej niż 128
8.	Wydajność Firewall	nie mniej niż 7,7 Gbps
9.	Wydajność Firewall IMIX	nie mniej niż 3,5 Gbps
10.	Wydajność IPS	nie mniej niż 2 Gbps
11.	Wydajność FW+IPS+AV	nie mniej niż 0,685 Gbps
12.	Wydajność NGFW	nie mniej niż 2 Gbps
13.	Liczba równoczesnych połączeń	nie mniejsza niż 1600000
14.	Liczba nowych połączeń na sekundę	nie mniejsza niż 61500
15.	Wydajność IPsec VPN	nie mniej niż 3,6 Gbps
16.	Wydajność dla inspekcji ruchu SSL/TLS	nie mniej niż 0,65 Gbps
17.	Liczba równoczesnych połączeń SSL/TLS	nie mniejsza niż 8192
18.	Liczba równoczesnych tuneli SSL VPN	nie mniejsza niż 1250
19.	Liczba równoczesnych tuneli IPsec VPN	nie mniejsza niż 750
20.	Zarządzanie	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym.

		Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter. Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. Rozwiązanie powinno oferować wiersz poleceń dostępny z poziomu graficznego interfejsu administratora, portu konsolowego oraz za pośrednictwem protokołu SSH z uwierzytelnianiem przy użyciu kluczy RSA, DSA lub ECDSA o długości min. 2048 bitów. Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm

		dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog). Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej. System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS). Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta. System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpowiednika). System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia. System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta, przy czym w podstawowej wersji utrzymywany i udostępniany jest on bezpłatnie i nie wymaga zakupu osobnych subskrypcji. Wymagane jest, aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP, via email jak i dodatkowo do centralnego systemu zarządzania w chmurze. Rozwiązanie powinno oferować wbudowany mechanizm pozwalający na automatyczne tworzenie szyfrowanych hasłem kopii zapasowych konfiguracji w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu. Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich. Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej. Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu licencyjnego a synchronizacja subskrypcji powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). Informacja o dostępności nowej wersji powinna pojawiać się w Web GUI.

		Producent powinien oferować mechanizm automatycznego łatania wykrytych w oprogramowaniu systemowym podatności przez tzw. hotfixies, przy czym administrator powinien móc funkcjonalność tą wyłączyć. Rozwiązanie powinno oferować mechanizm szyfrowania danych takich jak loginy, hasła, klucze które przechowywane są w konfiguracji urządzenia. Dane powinny być zabezpieczone dedykowanym kluczem szyfrującym tworzonym na podstawie bezpiecznie składowanego poza urządzeniem hasła. Rozwiązanie powinno zapewniać możliwość zmiany nazw interfejsów sieciowych.
21.	Zapora sieciowa	Wymagane jest, aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection. System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6. Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas. System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. System powinien pozwalać na selektywne wyłączanie reguł zapory sieciowej (bez konieczności ich usuwania). System powinien pozwalać na grupowanie reguł zapory. Wymagana jest funkcjonalność automatycznego wiązania nowotworzonych reguł do właściwych grup na podstawie kryteriów opisujących grupę. Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. System ochrony powinien zawierać predefiniowane strefy zapory typu: LAN, WAN, DMZ, VPN. Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej. System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). Rozwiązanie powinno oferować narzędzie do symulowanego testu reguł zapory w oparciu o zadane przez administratora kryteria takie jak IP, strefa zapory, użytkownik, dzień, godzina. System powinien pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika.
22.	Trasowanie ruchu	Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing. Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.

		Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów. Rozwiązanie powinno umożliwiać rozkładanie ruchu w oparciu o wagi interfejsów WAN. Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast. Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM). Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6.
23.	Translacja adresów i portów	Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT. Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT Rozwiązanie powinno pozwalać na automatyczne tworzenie reguł NAT typu loopback czy reflexive rule.
24.	Kształtowanie pasma i jakość usług	System powinien zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji. Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne. System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6. Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet (od 1 Business Critical do 7 Best Effort).
25.	Podstawowa ochrona przed atakami DoS i DDoS	System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
26.	Pozostałe	Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge). System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.

		System powinien oferować wsparcie dla IEEE 802.1Q VLAN z możliwością konfiguracji niezależnych puli DHCP. Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). System powinien oferować wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp. Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd). Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo). Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych.
27.	Kontroler sieci bezprzewodowej	System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania. Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Access Point, Wireless Bridge oraz Wireless Repeater. Uruchomienie punktów dostępowych sieci bezprzewodowej powinno odbywać się na zasadzie plug-and-play, gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu. Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej. Rozgłaszane sieci bezprzewodowe powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując przy tym możliwość izolacji klientów sieci bezprzewodowej. Rozwiązanie powinno umożliwiać rozgłaszanie wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej (Hide SSID). Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise. Rozwiązanie powinno zapewniać wsparcie dla uwierzytelniania klientów w oparciu o IEEE 802.1X (RADIUS Authentication). Rozwiązanie powinno oferować wsparcie dla IEEE 802.11r (Fast Transition). System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów. Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości.

		System powinien zapewniać możliwość tworzenia odseparowanej sieci dla gości w wariancie walled garden. System powinien pozwalać na rozgłaszanie sieci bezprzewodowych w oparciu o harmonogramy czasowe. Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych (Rogue AP detection).
28.	Uwierzytelnianie i obsługa użytkowników	Wymagane uwierzytelnianie użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta. Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników. System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+. Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory. System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm). Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server. System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu.
29.	Koncentrator VPN	System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2.

		System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519). System musi obsługiwać połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN. Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN. Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback. Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego. Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth. Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN. Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN. Urządzenie musi obsługiwać połączenia L2TP over IPsec. Połączenia VPN terminowane muszą być dedykowanej strefie zapory sieciowej.
30.	Logowanie i raportowanie	System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym. System powinien umożliwiać składowanie oraz archiwizację logów. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali. System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących. Rozwiązanie powinno umożliwiać wysyłanie raportów via email. Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV. Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog. System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.

		System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację. Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach. System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.
31.	Intrusion Prevention System i Advanced Threat Protection	Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur. Wymagane jest, aby system automatycznie aktualizował sygnatury zagrożeń. Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS. Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS. System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet.
32.	Ochrona i kontrola web - Ochrona przez Malware	Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP. Rozwiązanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania. Dodatkowo rozwiązanie powinno umożliwiać uruchomienie silnika antywirusowego firmy trzeciej. Wymagane jest, aby system automatycznie aktualizował sygnatury zagrożeń. System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek. Rozwiązanie musi przeprowadzać emulację skryptów Java. Rozwiązanie powinno przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta. Rozwiązanie powinno umożliwiać blokowanie potencjalnie niechcianych aplikacji (tzw. Potentially Unwanted Applications - PUAs) System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates)
33.	Inspecja ruchu SSL/TLS	Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów. Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2. Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP.

		Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443). Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web. Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen.
34.	Filtr Web	Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron Web oraz umożliwiać dodawanie własnych kategorii stron. Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy. Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól. System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowano treści komunikatu w tym dodania logo organizacji. Rozwiązanie powinno umożliwiać filtrowanie stron web analizując ich zawartość wykorzystując tzw. Content Filtering na bazie haseł kluczowych. Rozwiązanie powinno oferować ochronę przed Pharmingiem.
35.	Ochrona i kontrola aplikacji	Rozwiązanie powinno oferować bazę danych opisująca co najmniej 3000 aplikacji. Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji. Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji. Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów. Rozwiązanie powinno umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp. Rozwiązanie powinno oferować funkcje CASB (Cloud Access Security Broker) celem monitorowania i regulowania dostępu do aplikacji chmurowych wykorzystywanych przez użytkowników. Rozwiązanie powinno umożliwiać tworzenie własnych grup aplikacji co najmniej na potrzeby polityk SD-WAN.
36.	Ochrona przed nieznanymi zagrożeniami	Rozwiązanie klasy Sandbox do ochrony przez zagrożeniami typu Zero-Day.

		Rozwiązanie oferujące statyczną i dynamiczną analizę kodu przesyłanego w ramach ruchu web czy email. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf. Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab. System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS. System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu. System zapewniający analizę struktury kodu w tym analizę przeprowadzaną przez mechanizmy głębokiego uczenia maszynowego. System zapewniający ochronę przed exploitami i złośliwym kodem ransomware. System badający reputację pliku w zewnętrznych bazach takich jak np. Virustotal. System powinien oferować szczegółowe raporty dowodzące przeprowadznie analizy dla w/w mechanizmów.

3.Przełączniki sieciowe – 18 szt.

Minimalne wymagania oferowanego sprzętu:

- Przepustowość: 128 Gbps
- Szybkość przesyłania w Mpps (pakiety 64 bajtowe): 120
- Porty 10/100/1000: 24
- Porty uplink: 4 SFP+
- Porty obsługujące PoE+ (802.3af/at): 24
- Port konsoli: tak
- Port USB: tak
- Port zarządzania pozapasmowego: tak
- Wielkość tablicy MAC: 16K
- Wielkość pamięci flash: 128 MB
- DRAM: 512 MB
- VLANy: 4 tys.

- Sieci VLAN oparte na portach: 4 tys.
- Kolejki priorytetowe QoS: 8
- PVRST: 32
- Przychodzące/wychodzące listy ACL: 128
- Wpisy ARP: 512
- Statyczne wpisy ARP: 512
- Trasy statyczne: 64
- Routing dynamiczny: 512
- Policy Base Automation: tak
- QoS:
  - Mapowanie ACL i oznaczanie ToS/DSCP
  - Mapowanie ACL dla 802.1p
  - Mapowanie ACL do kolejek priorytetowych
  - Obsługa DiffServ
  - Zarządzanie kolejką priorytetową przy użyciu metod Wieght Round Robin (WRR), Strict Priority (SP) oraz połączenie WRR i SP
- Zarządzanie ruchem:
  - Zasady ograniczania prędkości połączeń przychodzących oparte na ACL
  - Ograniczenie prędkości transmisji, multicast i uknown unicast
  - Ograniczenie prędkości przychodzących na port
  - Ograniczenie szybkości połączeń wychodzących na port/kolejkę
- Bezpieczeństwo:
  - Uwierzytelnianie 802.1x
  - Uwierzytelnianie MAC
  - DHCP snooping
  - Uwierzytelnianie/autoryzacja poprzez RADIUS
  - Secure shell
  - Bezpieczna kopia (SCP)
  - Lokalna nazwa użytkownika/hasło
- Zestaw funkcji warstwy 2:
  - 802.1d
  - Uwierzytelnianie 802.1x
  - Auto MDI/MDIX
  - BPDU Guard, Root Guard
  - IGMP Snooping v1/v2/v3
  - LLDP/LLDP MED
  - IGMP Proxy
  - Statyczny MAC
  - Port Mirroring: port based, ACL based, VLAN based
  - Izolacja portów/Privet VLAN Edge
  - Link Aggregation Group (Static/LACP)
  - Rate Limiting/Storm Control
  - Jumbo frame: 9K

- DHCP Snooping
- Filtrowanie BPDU
- Ochrona przed atakami typu DoS
- Ping/TraceRoute/ICMPv6
- Zestaw funkcji warstwy 3:
- Routing pomiędzy VLAN
- Statyczne ARP
- Trasy statyczne
- Przekazywanie DHCP
- Routing dynamiczny: RIPv1/v2, OSFPv2
- Redystrybucja tras
- Zarządzenia:
- Kontroler chmurowy
- Standardowy interfejs wiersza poleceń (CLI)
- DHCP client
- Wbudowane sieciowe zarządzenia (HTTP/HTTPS)
- Wbudowany serwer DHCP
- SSH/SSHv2
- SNMP v1/v2/v3
- Przekazywanie DHCP
- Simpe Network Time Protocol (SNTP)
- Lokalny/zdalny system logowania
- TFTP/SFTP
- Telnet client/server
- Zarządzanie po IPv6
- Switching:
- Core Switching Features:
  - IEEE 802.1ab – Link Layer Discovery Protocol (LLDP)
  - IEEE 802.1D – Spanning tree compatibility
  - IEEE 802.1p – Ethernet priority with user provisioning and mapping
  - IEEE 802.1s – Multiple spanning tree compatibility
  - IEEE 802.1Q – Virtual LANs with port-based VLANs
  - IEEE 802.1X – port-base authentication
- VLAN Support:
  - IEEE 802.1W – Rapid spanning tree compatibility
  - IEEE 802.3 – 10BASE-T
  - IEEE 802.3u – 100BASE-T
  - IEEE 802.3ab – 1000BASE-T
  - IEEE 802.3ac – VLAN tagging
  - IEEE 802.3ad- Link aggregation
  - IEEE 802.3x – Flow control
- Parametry fizyczne:
- Zasilanie: 100-240 VAC

- Maksymalna moc przełącznika: 25,10W
- Waga: 3,96 kg
- Szybkość CPU: 800 MHz
- Budżet mocy PoE+: 400W
- Budżet mocy PoE per port: 30W
- Możliwość montażu w szafie: tak, 1U
- Zestaw do montażu w szafie rack: tak
- Wewnętrzne wentylatory: 2
- Zakres temperatur pracy: od 0°C do 50°C

4. UPS – 18 szt.
Minimalne wymagania oferowanego sprzętu:

Lp.	Parametry	Wymagania minimalne
1.	Nominalne napięcie wejściowe (Vac)	200
2.	Pojemność (VA)	1500
3.	Pojemność (Waty)	900
4.	Znamionowy prąd wejściowy (A)	10
5.	Rodzaj złącza wejściowego	IEC C14
6.	Rodzaj gniazdka	IEC C13 x 6
7.	Długość przewodu zasilania	1.83
8.	Ochrona przed przeciążeniem	Wewnętrzne ograniczenie prądu, bezpiecznik
9.	Czas pracy przy pełnym obciążeniu (min)	2,5
10.	Czas pracy przy połowie obciążenia (min)	11
11.	Konstrukcja obudowy	Metalowa
12.	Zaczepy typu rack	Tak
13.	Wykrywanie częstotliwości wejściowej	Automatyczne
14.	Gwarancja	3 lata

5. Wkładki optyczne – 72 szt.
Minimalne wymagania oferowanego sprzętu:

Lp.	Parametry	Wymagania minimalne
1.	Przepływność	Nie mniej niż 10 Gb
2.	Dystans	Nie mniej niż 0,3 km (300m)
3.	Medium transmisyjne	MultiMode
4.	Typ interfejsu	SFP+
5.	Długość fali TX	Nie mniej niż 850
6.	Typ złącza	LC/UPC
7.	Temperatura pracy	0|70
8.	Typ transmisji	Duplex
9.	Typ modułu	Duplex

6. Laptop – 2 szt
Minimalne wymagania oferowanego sprzętu

Lp.	Nazwa komponentu	Wymagane minimalne parametry
1.	Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych, min. 8 rdzeni, min. 16 wątków, min. 20MB cache, na poziomie wydajności liczonej w punktach min. 21300 pkt. w teście CPU Passmark-cpumarkt według wyników opublikowanych na http://www.cpubenchmark.net/cpu_list.php Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. ***Do oferty należy dołączyć wydruk ze strony: http://www.cpubenchmark.net potwierdzający spełnienie wymogów (dopuszcza się wydruk w języku angielskim).***
2.	Pamięć operacyjna RAM	Min. 16 GB 3200 MHz, DDR4
3.	Parametry pamięci masowej	Min. 32 GB Możliwość montażu dysku M.2 PCIe
4.	Karta graficzna	Karta o wydajności liczonej w punktach min. 17000 pkt. w teście Passmark G3D Mark według wyników opublikowanych na https://www.videocardbenchmark.net/high_end_gpus.html Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. ***Do oferty należy dołączyć wydruk ze strony: https://www.videocardbenchmark.net/ potwierdzający spełnienie w/w wymogu (dopuszcza się wydruk w języku angielskim).***

5.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki stereo, dwa mikrofony, kamera video min 1,0Mpix z zaślepką (zamawiający nie dopuszcza stosowania zaślepki wyprodukowanej przez innego producenta niż producent oferowanego urządzenia), sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute). Streamer z 1 x USB 3.2 Gen 1 (3.0/3.1 Gen 1), min. 1 slot na nośnik RDX, całkowita pojemność po kompresji 4 TB, całkowita pojemność natywna min. 2 TB.
6.	Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej. Umożliwiająca instalację dwóch dysków SSD.
7.	Zgodność z systemami operacyjnymi	Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym. ***Do oferty należy załączyć wydruk potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera (dopuszcza się dokument w języku angielskim).***
8.	Bezpieczeństwo	Zintegrowany z płytą główną układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego zapisanego w TPM. Dysk z zainstalowanym systemem operacyjnym zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
9.	Ekran	Matowy, matryca LED IPS Matowa min. 17,3” z podświetleniem w technologii LED, rozdzielczość FHD 1920x1080 (Full HD), Częstotliwość odświeżania ekranu 144Hz. Jasność min. 300cd/m2.
10.	Interfejsy / Komunikacja	Min. porty 4x USB z czego min. cztery porty USB 3.2 Min. jeden port USB-C, który musi umożliwiać ładowanie komputera i transmisję obrazu oraz podłączenie stacji dokującej, HDMI 2.1 , złącze ethernet RJ45 (nie może być uzyskane za pomocą przejściówek czy adapterów).
11.	Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AX + Bluetooth min. 5.0.
12.	Klawiatura	Wydzielona klawiatura numeryczna Wielodotykowy, intuicyjny Touchpad.
13.	Czytnik kart	Wbudowany czytnik kart pamięci.

14.	Napęd optyczny	Możliwość podłączenia nagrywarki DVD.
15.	Akumulator	Litowo-polimerowy.
16.	Zasilacz	Zasilacz zewnętrzny.
17.	Waga/Wymiary	Waga urządzenia z akumulatorem: max 2,98 kg. Grubość notebooka nie większa niż: 26,2 mm.
18.	System operacyjny	Microsoft Windows 11 Pro lub równoważny tj. system operacyjny klasy PC, który spełnia następujące minimalne wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim. 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe. 6. 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. 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.

		15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. 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.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM. 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot). 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło,

		b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN, e. Certyfikat/Klucz i uwierzytelnienie biometryczne. 39. Wsparcie dla uwierzytelniania na bazie Kerberos v.5. 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń. 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń. ***W przypadku zaoferowania systemu równoważnego do oferty należy załączyć oświadczenie producenta lub dokumentację techniczną potwierdzające posiadanie przez oferowany system równoważny co najmniej w/w funkcjonalności***
19.	Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.
20.	Gwarancja	Minimalny czas gwarancji producenta 36 miesięcy.
21.	Wsparcie techniczne producenta	▪ Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera. ▪ Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera. ▪ Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00. Wsparcie techniczne świadczone przez producenta lub autoryzowanego partnera serwisowego dla urządzeń i preinstalowanego oprogramowania OEM, zakupionego z urządzeniem, dostarczane zdalnie. Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta. Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.

7. Oprogramowanie wspierające zarządzanie urządzeniami sieciowymi UTM

Lp.	Nazwa komponentu	Minimalne wymagania
1.	Wyszukiwanie i przeglądanie dzienników systemowych	TAK
2.	Definiowanie raportów dotyczących zapór firewall	TAK
3.	Wdrażanie bezobsługowe poprzez chmurę IT	TAK
4.	Zarządzanie kopiami zapasowymi	TAK
5.	Zaplanowane aktualizacje oprogramowania sprzętowego	TAK
6.	Zarządzanie grupami zapór	TAK
7.	Raportowanie wielu zapór sieciowych	TAK
8.	Synchronizacja zasad zapory sieciowej grupy	TAK
9.	Dostęp przez aplikację mobilną	TAK
10.	Wykrywanie zagrożenia phisingiem	TAK
11.	Monitorowanie statusu połączenia VPN	TAK
12.	Zapewnienie pojemności do przechowywania logów z zarządzanych urządzeń	Łącznie 3400 GB przez okres 12 miesięcy

8. Modernizacja serwerowni i sieci LAN

W ramach niniejszego zostaną podjęte działania, które pozwolą zainstalować zakupione w ramach projektu urządzenia do serwerowni głównej oraz rezerwowej.

Modernizacja serwerowni głównej obejmie:

- zbudowanie ścianki działowej w pokoju informatyków w celu wydzielenia i zabezpieczenia serwerowni,
- montaż zamka elektronicznego na kartę lub kod,

Stan obecny serwerowni głównej
UWAGA: wymiary w centymetrach podane z dokładnością +- 10 cm

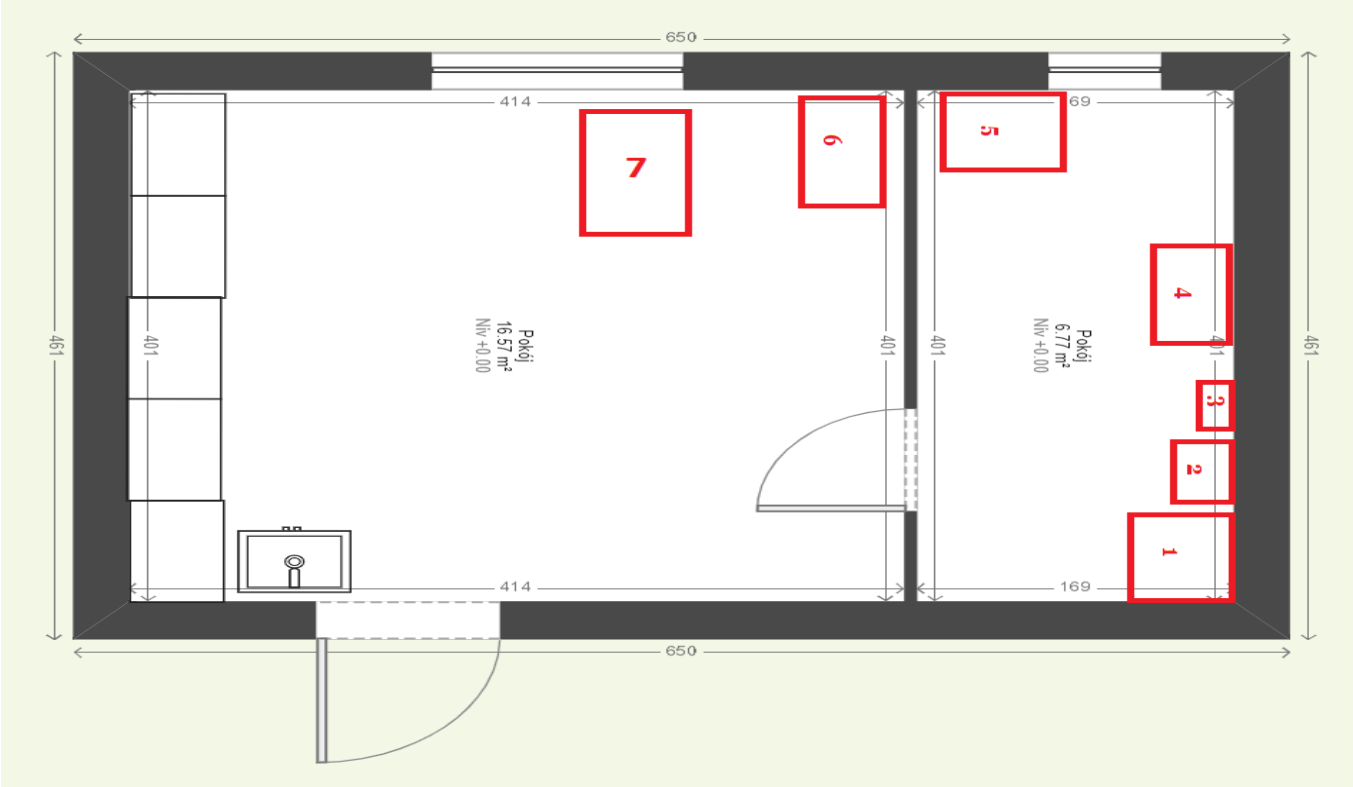
Wykonawca ma obowiązek samodzielnego wykonania pomiarów.

Przez cały okres prowadzonych prac w serwerowni znajdują się:
1. szafa stojąca 42 U z wyposażeniem głębokość 80 cm (3 switche, 1 router, 4 patchpanele, UPS, 1 UTM)
2. szafa wisząca 24 U z wyposażeniem głębokość 80 cm (1 switch, 1 UPS)
3. szafa wisząca 12 U głębokość 80 cm (1 router)
4. szafa stojąca 24U z wyposażeniem głębokość 100 cm (2 serwery, 2 ups, 1 switch, 1 router)
5. szafa stojąca 42U z wyposażeniem głębokość 100 cm (2 ups, 2 serwery, macierz)
6. szafa stojąca 24U z wyposażeniem głębokość 100 cm (1 serwer, 1 ups)
7. szafa stojąca 42U z wyposażeniem głębokość 100 cm (3 ups, 2 serwery, 1 macierz)

Serwery wraz z wyposażeniem są niezbędne do pracy Urzędu Miasta Pionki i muszą mieć zapewnione warunki do prawidłowego oraz nieprzerwanego działania w godzinach pracy urzędu, tj. 7:00 – 16.00.

Wykonawca ma obowiązek zabezpieczenia urządzeń w serwerowni przed zanieczyszczeniami związanymi z wykonywaną modernizacją. Wykonawca ustali sposób zabezpieczenia z Zamawiającym.

Stan obecny serwerowni głównej



Stan po modernizacji

Zakres prac

Praca	Zakres prac
Ścianka działowa	1. Demontaż obecnej ścianki działowej 2. Montaż nowej ścianki działowej • wymiary: 400 x 290 cm
Zamek elektryczny	1. Montaż zamka elektronicznego z dostępem za pomocą karty lub kodu
Montaż szafy teleinformatycznej 42U.	1. Przygotowanie miejsca na szafę 42U 2. Montaż punktów logicznych sieci komputerowej do podłączenia serwerów: • ułożenie ciągów kablowych • montaż 12 gniazd PEL kat. 6a lub 7 z okablowaniem

Dodatkowe prace	Ustawienie obecnie użytkowanych szaf w miejscach wskazanych przez Zamawiającego w utworzonym pomieszczeniu.

Parametry modernizowanych elementów i wymagania

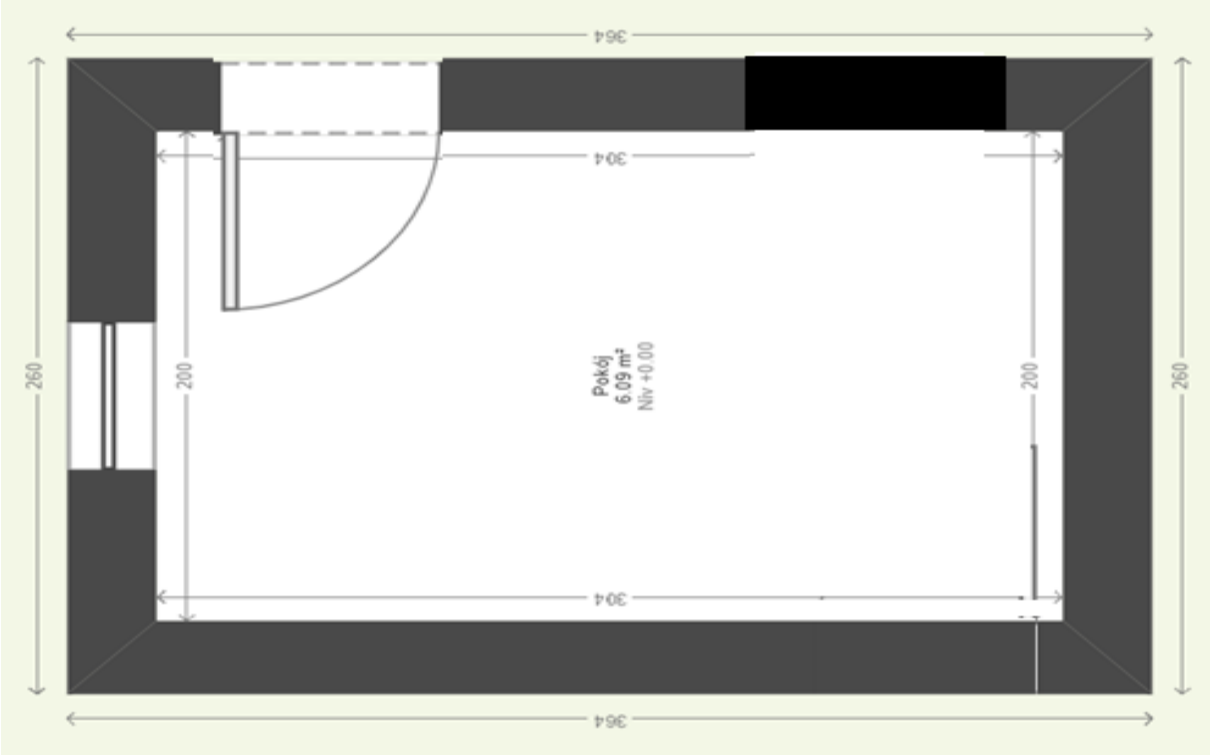
Komponent	Minimalne wymagania
Ścianka działowa	Demontaż ścianki: 1. Wykonawca zdemontuje obecną ściankę działową z płytami kartonowo gipsowymi, wypełnioną watą wygłuszającą oraz płytami 2. Wykonawca zatynkuje otwory w ścianach. Wzmocnienie podłogi: 1. Wykonawca dostarczy i ułoży na podłodze płytę OSB o grubości co najmniej 25 mm przeznaczoną do podłóg, zabezpieczoną przed wilgocią w całym pomieszczeniu – pokój 1 i pokój 2 2. Wykonawca dostarczy i ułoży na podłodze wykładzinę PCV w kolorystyce ustalonej z Zamawiającym, odporną na ogień w całym pomieszczeniu – pokój 1 i pokój 2 Montaż ścianki: 1. Wykonawca wykonana ściankę działową w konstrukcji szkieletowej wykończoną z obu stron płytą OSB 2. Wykonawca zamontuje drzwi • z pełnym skrzydłem • o wymiarach otworu nie mniejszych niż: szerokość 90cm, wysokość 200 cm • metalowych odpornych na uszkodzenia • z ościeżnicą, skrzydłem, klamką, wkładką budowlaną, zamkiem, uszczelką wytłumiającą 3. Wykonawca zamontuje kratkę/i wentylacyjną/e z żaluzjami (z możliwością zamknięcia) o powierzchni wlotu mnie mniejszej niż 20 cm2 4. Wykonawca pomaluje wykonaną ściankę farbą koloru białego odporną na ścieranie Wykonawca zdobędzie wszystkie zgody przewidziane prawem. Po zakończeniu prac Wykonawca dostarczy dokumentację techniczną i inwentaryzacyjną wymaganą prawem.
Zamek elektryczny	1. Dostarczony i zamontowany zamek musi zostać podłączony do systemu alarmowego Urzędu Miasta po

	uzgodnieniu z konserwatorem alarmu 2. Zamek musi umożliwiać otwarcie drzwi za pomocą karty lub kodu PIN 3. Zamek musi zostać skonfigurowany z centralą alarmową: • kody PIN dla 3 osób • karty dla 3 osób • rejestracja informacji o dacie, godzinie i osobie otwierającej drzwi
Punkty logiczne RJ45	Wykonawca wykona ciągi kablowe o następujących parametrach: 1. długość: 30 m 2. Korytko kablowe metalowe o wymiarach co najmniej 300mm x 60 mm 3. rozmieszczenie: pod sufitem Wykonawca wykona 12 punktów PEL Wykonawca musi posiadać osoby posiadające uprawnienia do montażu wskazanej instalacji.
Dodatkowe prace	Ustawienie obecnie użytkowanych szaf w miejscach wskazanych przez Zamawiającego w utworzonym pomieszczeniu.

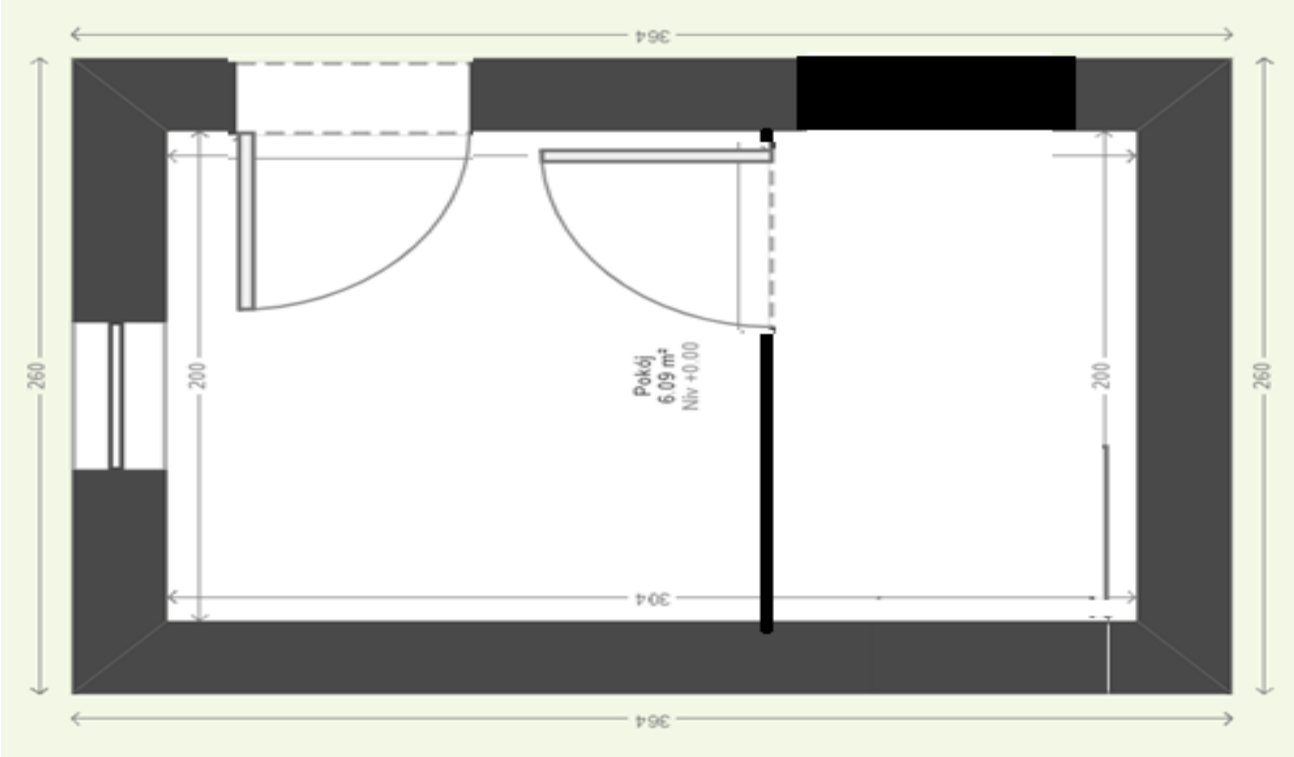
Modernizacja serwerowni rezerwowej obejmuje:

- zbudowanie ścianki działowej w pokoju informatyków w celu wydzielenia i zabezpieczenia serwerowni,
- montaż zamka elektronicznego na kartę lub kod,
- montaż szafy teleinformatycznej 42U, w tym montaż gniazd sieciowych.

Stan obecny serwerowni rezerwowej



Stan po modernizacji



Zakres prac budowlanych

Praca	Zakres prac
Ścianka działowa	1. Montaż nowej ścianki działowej • wymiary: 200 x 290 cm
Otwór drzwiowy	1. Wykonanie otworu drzwiowego
Zamek elektryczny	1. Montaż zamka elektronicznego z dostępem za pomocą karty lub kodu
Montaż szafy teleinformatycznej 42U.	1. Przygotowanie miejsca na szafę 2. Montaż punktów logicznych sieci komputerowej do podłączenia serwerów: • ułożenie ciągów kablowych • montaż 8 punktów PEL • montaż 6 gniazd światłowodowych połączonych z serwerownią główną
Dodatkowe prace	Ustawienie obecnie użytkowanych szaf w miejscach wskazanych przez Zamawiającego w utworzonym pomieszczeniu.

Parametry modernizowanych elementów i wymagania

Komponent	Minimalne wymagania
Ścianka działowa	Wzmocnienie podłogi: 1. Wykonawca dostarczy i ułoży na podłodze płytę OSB o grubości co najmniej 25 mm przeznaczoną do podłóg, zabezpieczoną przed wilgocią. 2. Wykonawca dostarczy i ułoży na podłodze wykładzinę PCV w kolorystyce ustalonej z Zamawiającym, odporną na ogień Montaż ścianki: 1. Wykonawca wykonana ściankę działową w konstrukcji szkieletowej wykończoną z obu stron płytą OSB 2. Wykonawca zamontuje drzwi • z pełnym skrzydłem • o wymiarach otworu nie mniejszych niż: szerokość 90cm, wysokość 200 cm • metalowych odpornych na uszkodzenia • z ościeżnicą, skrzydłem, klamką, wkładką budowlaną, zamkiem, uszczelką wytłumiającą 3. Wykonawca wykończy połączenia ściana-ścianka pianką 4. Wykonawca zamontuje kratkę/i wentylacyjną/e z żaluzjami (z możliwością zamknięcia) o powierzchni wlotu mnie mniejszej niż 40 cm2 5. Wykonawca pomaluje wykonaną ściankę farbą koloru białego odporną na ścieranie Wykonawca zdobędzie wszystkie zgody przewidziane prawem. Po zakończeniu prac Wykonawca dostarczy dokumentację techniczną i inwentaryzacyjną wymaganą prawem.
Zamek elektryczny	1. Dostarczony i zamontowany zamek musi zostać podłączony do systemu alarmowego Urzędu Miasta po uzgodnieniu z konserwatorem alarmu 2. Zamek musi umożliwiać otwarcie drzwi za pomocą karty lub kodu PIN 3. Zamek musi zostać skonfigurowany z centralą alarmową: 1. kody PIN dla 3 osób 2. karty dla 3 osób 3. rejestracja informacji o dacie, godzinie i osobie otwierającej drzwi
Punkty logiczne RJ45 i FC	Wykonawca wykona ciągi kablowe o następujących parametrach: 1. długość: 60 m z serwerowni głównej 2. Korytko kablowe metalowe o wymiarach co najmniej 300mm x 60 mm

	3. rozmieszczenie: pod sufitem Wykonawca wykona 8 punktów PEL z serwerowni głównej o następujących parametrach: 1. kategorii 6a lub 7 2. długość okablowania pojedynczego punktu: 80 m. Wykonawca wykona montaż 6 gniazd światłowodowych połączonych z serwerownią główną Wykonawca musi posiadać osoby posiadające uprawnienia do montażu wskazanej instalacji.
Dodatkowe prace	Ustawienie obecnie użytkowanych szaf w miejscach wskazanych przez Zamawiającego w utworzonym pomieszczeniu.

Wykonawca zobowiązany jest do:

1. przeprowadzenia wizji lokalnej
2. ustalenia z Zamawiającym zakresu prac i rozmieszczenia elementów
3. przygotowania harmonogramu prac
4. przygotowania dokumentacji powykonawczej
5. przekazania Zamawiającemu praw autorskich do dokumentacji powykonawczej