Znak sprawy:

Załącznik Nr 5 do zapytania ofertowego

Szczegółowy opis przedmiotu zamówienia (SOPZ)

Część I zamówienia: Serwer z oprogramowaniem

Serwer powinien spełniać następujące wymagania:

- minimum dwa procesory
- liczba rdzeni każdego z procesorów nie mniej niż 8
- każdy z procesorów powinien osiągnąć minimum 12 tys. pkt. w testach dostępnych na stronie https://www.cpubenchmark.net
- ilość pamięci ram nie mniejsza niż 64GB DDR4
- zamontowane dyski: - 2 szt. SSD klasy enterprise min, 480GB każdy oraz 3 szt SAS 10k min. 900GB każdy
- kontroler RAID pozwalający na zbudowanie RAID: 0,1,10,5,50,6,60
- minimum 4 karty sieciowe Gigabitowe
- serwer musi posiadać minimum dwa zasilacze
- system windows server 2019 (licencja bezterminowa)
- wymagane są szyny do zamocowania serwera w szafie RACK 19"
- okres gwarancji min. 60 miesięcy w trybie D2D, serwis gwarancyjny urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.

Dostarczony serwer powinien mieć stworzone dwie macierze RAID, tj. RAID1 stworzony z 2 dysków SSD oraz RAID5 stworzony z 3 dysków SAS. Serwer powinien mieć zainstalowany system operacyjny windows server 2019 w wersji umożliwiającej pracę 20 użytkownikom, zgodnie z licencjonowaniem firmy Microsoft oraz umożliwiać zainstalowanie minimum 1 maszyny wirtualnej.

Część II: Antywirus wersja serwerowa; oprogramowanie do monitorowania sieci

Antywirus wersja serwerowa

1. Kompletny pakiet bezpieczeństwa dla stacji roboczych, urządzeń mobilnych i serwerów plikowych - 20 stanowisk na 36 miesięcy.
2. Możliwość zarządzania z lokalnej konsoli lub usługi chmurowej.
3. Możliwość zdalnego zainstalowania oprogramowania zabezpieczającego na stacjach roboczych oraz pełny pogląd stanu ochrony sieci i zabezpieczonych urządzeń.

4. Możliwość automatycznego wysyłania powiadomień e-mail po wystąpieniu zdarzenia o wybranym poziomie szczegółowości.
5. Zabezpieczenie stacji roboczych:
   a) dwukierunkowy firewall,
   b) kontrola dostępu do stron WWW,
   c) ochrona przed botnetami.
   d) ochrona systemu plików w czasie rzeczywistym — wszystkie pliki w momencie otwarcia, utworzenia lub uruchomienia na komputerze są skanowane w poszukiwaniu szkodliwego kodu,
   e) kontrola dostępu do urządzeń — udostępnione funkcje automatycznej kontroli korzystania z urządzeń (CD, DVD, USB...). Przy użyciu tego modułu można blokować i dostosowywać rozszerzone filtry i uprawnienia oraz określać uprawnienia dostępu użytkowników do danego urządzenia i pracy z nim,
   f) system monitorujący zdarzenia występujące wewnątrz systemu operacyjnego i reagujący na nie zgodnie z odpowiednio dostosowanym zestawem reguł,
   g) skaner pamięci działający w połączeniu z blokadą programów typu Exploit w celu wzmocnienia ochrony przed szkodliwym oprogramowaniem, które unika wykrycia przez produkty do ochrony przed szkodliwym oprogramowaniem poprzez zastosowanie zaciemniania kodu i/lub szyfrowania,
   h) blokada programów typu Exploit —wzmocnienie ochrony typów aplikacji będących często celami ataków, takich jak przeglądarki internetowe, przeglądarki plików PDF, programy poczty e-mail oraz składniki pakietu MS Office, skaner skryptów AMSI,
   i) ochrona przed oprogramowaniem wymuszającym okup,
   j) tryb prezentacji,
   k) skanowanie całego ruchu sieciowego wykorzystującego protokoły HTTP i HTTPS w poszukiwaniu szkodliwego oprogramowania.
   l) monitorowanie komunikacji przy użyciu protokołów POP3 i IMAP.
   m) ochrona przed atakami typu „phishing” — chroni użytkownika przed próbami pozyskania haseł, danych bankowych lub innych poufnych informacji przez nielegalnie działające strony internetowe podszywające się pod strony internetowe uprawnione do pozyskiwania tego rodzaju informacji.
   n) Filtr antyspamowy,
   o) Obsługa systemów operacyjnych: Microsoft Windows 11, Microsoft Windows 10, Microsoft Windows 8.1, 8, Microsoft Windows 7, OS, Ubuntu Desktop 18.04 LTS 64-bit, Ubuntu Desktop 20.04 LTS 64-bit, SUSE Linux Enterprise Desktop 15, Red Hat Enterprise Linux 7 64-bit z zainstalowanym obsługiwanym środowiskiem pulpitu (obsługiwane środowiska pulpitu: GNOME, KDE, XFCE).
6. Ochrona urządzeń mobilnych:
   a) aplikacja do ochrony urządzeń mobilnych, chroniąca w czasie rzeczywistym wszystkie aplikacje i pliki użytkownika, zainstalowane na tabletach i smartfonach.
   b) funkcja antyphishing chroniąca przed fałszywymi stronami internetowymi, które próbują wyłudzić hasła i dane logowania.

c) kontrola aplikacji wprowadzająca polityki bezpieczeństwa dla urządzeń mobilnych i pozwalająca ustalać, które aplikacje mogą być instalowane przez użytkownika na urządzeniach mobilnych.
d) Obsługa systemu Android w wersji 5 i nowszej.
7. Ochrona serwerów plikowych:
a) ochrona antywirusowa i antyspyware dla serwerów plików,
b) zabezpieczanie przed wszystkimi rodzajami zagrożeń, m.in. przed wirusami, rootkitami, robakami i oprogramowaniem szpiegującym,
c) skaner pamięci rozbudowujący ochronę antywirusową o skuteczne zabezpieczenie przed skomplikowanymi zagrożeniami, wielokrotnie spakowanymi lub zaszyfrowanymi,
d) możliwość skanowania z wykorzystaniem chmur,
e) faza przed uruchomieniem korzysta z technologii takich jak skaner UEFI,
f) wbudowany sandbox, sygnatury DNA,
g) blokada programów
h) typu Exploit, ochrona przed oprogramowaniem wymuszającym okup, zaawansowany skaner pamięci i skaner skryptów AMSI,
i) skanowanie dysków maszyn wirtualnych na serwerze funkcji Microsoft Hyper-V bez konieczności wcześniejszej instalacji „agenta" na danej maszynie wirtualnej,
j) możliwość jednoczesnego przeprowadzenie kilku skanowań środowiska Hyper-V,
k) automatyczne wykrywanie i wyłączanie najważniejszych aplikacji oraz plików serwera w celu zapewnienia płynnego działania i wysokiej wydajności,
l) wyłączenie określonych procesów ze skanowania w poszukiwaniu szkodliwego oprogramowania przy dostępie,
m) Obsługa systemów operacyjnych:

– Microsoft Windows Server 2008 (x86 and x64), 2008 R2, 2012, 2012 R2, 2016, 2019
– Microsoft Windows Storage Server 2008 R2 Essentials SP1, 2012, 2012 R2
– Microsoft Windows Small Business Server 2003 (x86), 2003 R2 (x86), 2008 (x64), 2011 (x64)
– Microsoft Windows Server 2012 Essentials, 2012 R2 Essentials
– Microsoft MultiPoint Server 2010, 2011
– Windows MultiPoint Server 2012
– Linux – kernel version 2.6.x lub nowszy; biblioteka glibc 2.3.6 lub nowsza
– Dazuko kernel moduł 2.0.0 lub nowszy (opcjonalnie)
– FreeBSD – Version 9.x
– NetBSD – Version 4.x
– Sun Solaris – Version 10

Oprogramowanie do monitorowania sieci

Licencja do monitorowania sieci LAN, zarządzania użytkownikami, zarządzania zasobami IT i helpdesku dla pracowników Urzędu ma obejmować 18 stacji roboczych. W ramach licencji producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne na okres minimum 12 miesięcy. Oprogramowanie ma zawierać centralną konsolę do zarządzania instalowaną lokalnie. Oprogramowanie ma zawierać funkcje takie jak:

- skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP
- interaktywne mapy sieci, mapy użytkownika, oddziałów, mapy inteligentne
- jednoczesna praca wielu administratorów, zarządzanie uprawnieniami, dzienniki dostępu
- serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/utraconych pakietów (PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.)
- liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków, transfer sieciowy itp.
- działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń
- liczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne)
- kompilator plików MIB
- obsługa pułapek SNMP
- routery i switche: mapowanie portów
- obsługa komunikatów syslog
- alarmy zdarzenie - akcja
- powiadomienia (pulpitowe, e-mail, SMS) oraz akcje korekcyjne (uruchomienie programu, restart komputera itp.)
- raporty (dla urządzenia, oddziału, wybranej mapy lub całej sieci)
- tworzenie zgłoszeń serwisowych i zarządzanie nimi (przypisywanie do administratorów)
- komentarze, zrzuty ekranowe i załączniki w zgłoszeniach
- konfigurowanie pól niestandardowych, powiązanych w wybraną kategorią zgłoszenia
- automatyzacje bazujące na założeniu: warunek-> akcja
- przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o Sygnalistach")
- dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę
- dwa tryby widoku - jasny i ciemny
- planowanie zastępstw w przydzielaniu zgłoszeń
- rozbudowany system raportów
- powiadomienia i widok zgłoszenia odświeżany w czasie rzeczywistym
- baza zgłoszeń z rozbudowaną wyszukiwarką
- baza wiedzy z kategoryzacją artykułów i możliwością wstawiania grafik oraz filmów z YouTube
- przejrzysty i intuicyjny interfejs webowy
- wewnętrzny komunikator (czat) z możliwością przydzielania uprawnień oraz przesyłania plików i tworzenia rozmów grupowych

- komunikaty wysyłane do użytkowników/komputerów z możliwym/obowiązkowym potwierdzeniem odczytu
- zdalny dostęp do komputerów z możliwością blokady myszy/klawiatury
- dwukierunkowa wymiana plików
- zarządzanie procesami Windows z poziomu okna informacji o urządzeniu
- zadania dystrybucji oraz uruchamiania plików (zdalna instalacja oprogramowania)
- procesowanie zgłoszeń z wiadomości e-mail
- integracja bazy użytkowników z Active Directory
- zarządzanie kontami lokalnych użytkowników Windows (tworzenie, usuwanie, edycja, reset hasła, eskalacja/deeskalacja uprawnień oraz włączanie/wyłączanie kont).
- audyt inwentaryzacji sprzętu i oprogramowania
- wgląd w licencje przypisane do użytkownika pracującego na wielu urządzeniach
- zdalny dostęp do managera plików z możliwością usuwania plików użytkownika
- informacje o wpisach rejestrowych, plikach i archiwach .zip na stacji roboczej
- szczegółowe informacje o konfiguracji sprzętowej konkretnej stacji roboczej
- zarządzanie instalacjami/dezinstalacjami oprogramowania w oparciu o menedżera pakietów MSI
- alarmy: instalacja oprogramowania, zmiana w zasobach sprzętowych
- lista kluczy oprogramowania Microsoft
- aplikacja dla systemu Android umożliwiająca spis z natury na bazie kodów kreskowych, kodów QR
- możliwość archiwizacji i porównywania audytów
- monitorowanie harmonogramu zadań Windows
- redukcja kosztów wydruku
- blokowanie stron WWW
- blokowanie uruchamianych aplikacji
- monitorowanie wiadomości e-mail (nagłówki) - antyphishing
- szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy)
- użytkowane aplikacje (aktywnie i nieaktywnie)
- odwiedzane strony WWW (tytuły i adresy stron, liczba i czas wizyt)
- audyty wydruków (drukarka, użytkownik, komputer), koszty wydruków
- użycie łącza: generowany przez użytkowników ruch sieciowy
- statyczny zdalny podgląd pulpitu użytkownika (bez dostępu)
- zrzuty ekranowe (historia pracy użytkownika ekran po ekranie)
- blokowanie uruchamiania procesów na podstawie lokalizacji pliku .EXE
- zarządzanie regułami blokowania aplikacji i stron WWW (tworzenie, grupowanie, powielanie między grupami użytkowników)

Część III zamówienia – UTM + licencje; Switch 48 port; Stacje robocze; System do backup

<u>UTM urządzenie +oprogramowanie</u>

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

a) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
b) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
c) Monitoring stanu realizowanych połączeń VPN.
d) System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

a) System realizujący funkcję Firewall musi dysponować minimum:
– 4 portami Gigabit Ethernet RJ-45.
b) System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
c) W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
d) System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

a) W zakresie Firewall'a obsługa nie mniej niż 100 tys. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.
b) Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
c) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps.
d) Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.
e) Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.
f) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
g) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 400 Mbps.

Funkcje Systemu Bezpieczeństwa:
W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
b) Kontrola Aplikacji.
c) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
d) Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
e) Ochrona przed atakami - Intrusion Prevention System.
f) Kontrola stron WWW.
g) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
h) Zarządzanie pasmem (QoS, Traffic shaping).
i) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
j) Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
k) Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
l) Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall
a) Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
b) System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   – Translację jeden do jeden oraz jeden do wielu.
   – Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
c) W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
d) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
e) Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   – Amazon Web Services (AWS).
   – Microsoft Azure
   – Google Cloud Platform (GCP).
   – OpenStack.
   – VMware NSX.

Połączenia VPN
a) System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
– Wsparcie dla IKE v1 oraz v2.
– Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
– Obsługa protokołu Diffie-Hellman grup 19 i 20.

- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
  - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
  - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
  - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
  - Mechanizm „Split tunneling" dla połączeń Client-to-Site.

b) System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
- Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

- Routingu statycznego.
- Policy Based Routingu.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres **24 miesięcy.**

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres **12** miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7

Switch 48 port gigabitowy

- **Sieć - Standardy komunikacyjne:** IEEE 802.1D,IEEE 802.1Q,IEEE 802.1ab,IEEE 802.1p,IEEE 802.1w
- **Sieć - Automatyczne MDI/MDI-X:** Tak
- **Sieć - Auto-Negocjacja:** Tak
- **Sieć - Obsługa sieci VLAN:** Tak
- **Sieć - Liczba VLANs:** 4094
- **Cechy zarządzania - Typ przełącznika:** Zarządzany
- **Cechy zarządzania - Zarządzany w chmurze:** Tak
- **Warstwa przełącznika:** L2
- **Wbudowany wiatrak:** Niewymagany
- **Konstrukcja - Możliwości montowania w stelażu:** Tak
- **Konstrukcja - Układ:** 1U
- **Konstrukcja - Diody LED:** Tak
- **Porty i interfejsy - Podstawowe przełączanie RJ-45 Liczba portów Ethernet:** min. 48
- **Porty i interfejsy - Podstawowe przełączania Ethernet RJ-45 porty typ:** Gigabit Ethernet (10/100/1000)
- **Porty i interfejsy - Liczba zainstalowanych modułów SFP:** min. 2
- **Moc - Zasilacz dołączony:** Tak
- **Warunki pracy - Zakres temperatur (eksploatacja):** 0 - 40 °C
- **Warunki pracy - Zakres wilgotności względnej:** 5 - 95%
- **Moc - Napięcie wejściowe AC:** 100 - 240 V
- **Moc - Częstotliwość wejściowa AC:** 47/63 Hz
- **Przesyłanie danych - Przepustowość rutowania/przełączania:** min. 100 Gbit/s
- **Przesyłanie danych - Wielkość tabeli adresów:** min. 32000 wejścia
- **Przesyłanie danych - Liczba kolejek:** min. 8
- **Zestaw do montażu haków:** Tak

Stacje robocze – 5 szt. :

L.p.	PARAMETRY	CHARAKTERYSTYKA (wymagania minimalne bądź lepsze)
1.	OBUDOWA	Dowolny rodzaj; Wyposażona w czytnik kart multimedialnych; Obudowa trwale oznaczona nazwą producenta
2.	PŁYTA GŁÓWNA	Zaprojektowana i wyprodukowana przez producenta komputera. Wyposażona w złącza min.: - 1 x PCI Express 3.0 x16, - 1 x PCI Express 3.0 x1,
3.	PROCESOR	Min. 8500 pkt na stronie testowej https://www.cpubenchmark.net
4.	PAMIĘĆ RAM	DDR4 Minimum: 8GB z możliwością rozszerzenia do min, 64 GB Ilość wolnych banków pamięci: min. 1 szt.
5.	DYSK	min. 512GB SSD(możliwy M.2)
6.	PORTY/ZŁĄCZA	Przedni panel: min. 1 x Czytnik kart pamięci, 1x Wyjście słuchawkowe/wejście mikrofonowe, 4x USB 3.0 Typ-A Panel tylni: min. 1x RJ-45, 1x RS-232, 1x VGA, 4x USB 2.0, 1x HDMI, 1x wyjście liniowe, 1x wejście liniowe, 1x złącze zasilania,
7.	ŁĄCZNOŚĆ	Wi-Fi 5 (802.11 ac), Bluetooth 4.2, LAN 10/100/1000 Mbps
8.	KARTA GRAFICZNA	zintegrowana
9.	ZAINSTALOWANY SYSTEM OPERACYJNY	Windows 10/11 w wersji pro. Nie dopuszcza się licencji pochodzącej z rynku wtórnego
10.	NAPĘD OPTYCZNY	Nagrywarka DVD
11.	GWARANCJA	24 miesiące
12.	STAN	Produkt nowy
13.	ZAINSTALOWANE OPROGRAMOWANIE BIUROWE	Oprogramowanie musi spełniać następujące minimalne parametry: • Dostawa pełnej polskiej wersji językowej interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. Pakiet

		powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim. Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach pracy – cena połączenia nie większa niż cena połączenia lokalnego. Publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 5 lat od daty zakupu. Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0). b. Zintegrowany pakiet aplikacji biurowych musi zawierać co najmniej: o edytor tekstów, o arkusz kalkulacyjny, o narzędzie do przygotowania i prowadzenia prezentacji, • Edytor tekstów musi umożliwiać co najmniej: o Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. o Wstawianie oraz formatowanie tabel. o Wstawianie oraz formatowanie obiektów graficznych. o Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). o Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. o Automatyczne tworzenie spisów treści. o Formatowanie nagłówków i stopek stron. o Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. o Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. o Określenie układu strony (pionowa/pozioma). o Wydruk dokumentów. o Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. o Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. o Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy

		certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa. • Arkusz kalkulacyjny musi umożliwiać co najmniej: o Tworzenie raportów tabelarycznych. o Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych. o Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. o Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice). o Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. o Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych. o Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. o Wyszukiwanie i zamianę danych. o Wykonywanie analiz danych przy użyciu formatowania warunkowego. o Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. o Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. o Formatowanie czasu, daty i wartości finansowych z polskim formatem. o Zapis wielu arkuszy kalkulacyjnych w jednym pliku. o Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. • Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać co najmniej: o Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego. o Drukowanie w formacie umożliwiającym robienie notatek. o Zapisanie jako prezentacja tylko do odczytu. o Nagrywanie narracji i dołączanie jej do prezentacji. o Opatrywanie slajdów notatkami dla prezentera. o Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo. o Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego. o Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.

		○ Możliwość tworzenia animacji obiektów i całych slajdów. ○ Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. • Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: ○ Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego. ○ Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych. ○ Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców. ○ Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną. ○ Automatyczne grupowanie poczty o tym samym tytule. ○ Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy. ○ Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów. ○ Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie. ○ Zarządzanie kalendarzem. ○ Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników. ○ Przeglądanie kalendarza innych użytkowników. ○ Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach. ○ Zarządzanie listą zadań. ○ Zlecanie zadań innym użytkownikom. ○ Zarządzanie listą kontaktów. ○ Udostępnianie listy kontaktów innym użytkownikom. ○ Przeglądanie listy kontaktów innych użytkowników. ○ Możliwość przesyłania kontaktów innym użytkowników. LICENCJA DOŻYWOTNIA, WERSJA MOŻLIWA DO UŻYTKU W ADMINISTRACJI PUBLICZNEJ
14.	DODATKOWE WYPOSAŻENIE	Klawiatura i mysz przewodowa producenta, przewód zasilający
15.	MONITOR	Rodzaj podświetlania: LED Typ matrycy TFT lub IPS Rozmiar matrycy 24” Jasność 250 cd/m2

		Kontrast statyczny 1000:1 Kąty widzenia (pion/poziom) 178/178 stopni Częstotliwość odświeżania 75 Hz Czas reakcji matrycy (maksymalnie) 5ms (gray to gray) Rozdzielczość maksymalna 1920 x 1080 Złącza 1x VGA i 1x HDMI Możliwość montażu na ścianie – VESA 75x75 Głośniki nie są wymagane Klasa energetyczna min. E Dodatkowe wyposażenie: przewód zasilający; przewód wizyjny umożliwiający podłączenie do oferowanego komputera

System do backup

Sprzęt	
Procesor	
Model CPU	Klasy Intel Atom
architektura procesora	64-bit
Częstotliwość procesora	Czterordzeniowy min. 2.1 GHz
Mechanizm szyfrowania sprzętowego (AES-NI)	tak
Pamięć	
Pamięć systemowa	Min. 2 GB DDR4
Całkowita liczba gniazd pamięci	Min. 1
Przechowywanie	
Kieszeń/kieszenie na dyski	4
Maks. liczba kieszeni na dyski z jednostką rozszerzającą	8
Zgodny typ dysków	3.5" SATA HDD 2.5" SATA HDD 2.5" SATA SSD
Maksymalna pojemność wewnętrzna	64 TB (16 TB drive x 4)
Maksymalny rozmiar pojedynczego wolumenu	108 TB
Dysk z możliwością wymiany podczas pracy hot-swap	tak
Porty zewnętrzne	

Port LAN RJ-45 1GbE	4 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Port USB 3.0	2
port eSATA	1
PCIe	
Rozszerzenie karty PCIe	1 x Gen3 x8 slot (black, x4 link)
Obsługa karty dodatków	Karta sieciowa PCIeM2D18 - podwójna karta rozszerzeń M.2 SATA/NVMe SSD dla pamięci podręcznej SSD
System plików	
Wewnętrzne dyski twarde	Btrfs EXT4
Zewnętrzne dyski twarde	Btrfs EXT4 EXT3 FAT NTFS HFS+ exFAT HFS+
Uwagi	exFAT Access do nabycia osobno w Centrum pakietów.
Wygląd	
Obudowa (RU)	1U
Wentylator obudowy	3 szt.
Tryb prędkości wentylatora	Tryb pełnej prędkości Tryb chłodzenia Tryb cichy
Przywracanie zasilania	tak
Natężenie dźwięku	Maks. 30 dB(A)
Zaplanowane włączanie/wyłączanie	tak
Funkcja Wake on LAN/WAN	tak
Zasilacz / Adapter	Maks 250W
Napięcie wejściowe zasilania prądem zmiennym	100V do 240V AC
Częstotliwość zasilania	50/60 Hz, Jednofazowy
Zużycie energii	37,94 W (dostęp) 20.96 W (hibernacja dysków twardych

British thermal unit	129.54 BTU/hr (dostęp) 71.57 BTU/hr (hibernacja dysków twardych)
Temperatura otoczenia	
Temperatura pracy	0°C do 35°C (32°F do 95°F)
Temperatura przechowywania	-20°C do 60°C (-5°F do 140°F)
Wilgotność względna	5% do 95% RH
Certyfikaty	EAC VCCI CCC RCM KC FCC CE BSMI
Gwarancja	3-letnia gwarancja sprzętowa
Specyfikacje systemu DSM	
Zarządzanie przechowaniem	
Maks. liczba wolumenów wewnętrznych	64
Maksymalna liczba celów iSCSI	128
Maks. liczba jednostek LUN iSCSI	256
Migawka i LUN Clone iSCSI, Windows ODX	tak
Pamięć podręczna odczytu/zapisu na dyskach SSD	tak
SSD TRIM	tak
Obsługiwane typy macierzy RAID	Basic JBOD RAID 0 RAID 1 RAID 5 RAID 6 RAID 10
Migracja macierzy RAID	Basic to RAID 1 Basic to RAID 5 RAID 1 to RAID 5 RAID 5 to RAID 6
Powiększenie wolumenu za pomocą większych dysków twardych	Synology Hybrid RAID RAID 1 RAID 5

	RAID 6 RAID 10
Powiększenie wolumenu przez dodanie dysków twardych	Synology Hybrid RAID JBOD RAID 5 RAID 6 (z jednostką rozszerzającą)
Typy macierzy RAID obsługujące Hot Spare	Synology Hybrid RAID RAID 1 RAID 5 RAID 6 (z jednostką rozszerzającą) RAID 10 (z jednostką rozszerzającą)
Usługi plików	
Protokół plików	CIFS/AFP/NFS/FTP/WebDAV
Maks. liczba jednoczesnych połączeń protokołu CIFS/AFP/FTP	
Maks. liczba jednoczesnych połączeń protokołu CIFS/AFP/FTP (z rozbudową pamięci RAM)	2000
Integracja listy kontroli dostępu systemu Windows (ACL)	tak
Uwierzytelnienie NFS Kerberos	tak
Konto i folder współdzielony	
Maks. liczba lokalnych kont użytkowników	2048
Maks. liczba lokalnych grup	256
Maks. liczba folderów udostępnionych	512
Maks. liczba zadań synchr. folderów udostępnionych	8
Menedżer High Availability	tak
Centrum logów	tak
exFAT Access (opcjonalnie)	tak
Synology MailPlus / MailPlus Server	tak
Bezpłatne konta e-mail	5
Maksymalna liczba jednoczesnych użytkowników	150
Media Server	tak
Zgodność z DLNA	tak
Moments	tak
Rozpoznawanie twarzy	tak

Rozpoznawanie obiektów	tak
Automatyczny kolor & rotate	tak
Snapshot Replication	tak
Maksymalna liczba migawek na udostępniony folder	1024
Maksymalna liczba migawek systemu	65536
Virtual Machine Manager	tak
Zalecane instancje maszyn wirtualnych	4
Zalecana liczba maszyn Virtual DSM	4 (w tym 1 licencja bezpłatna)
VPN Server	tak
Maks. liczba połączeń	20

Oprogramowanie do backup
Konsola administratora

-Zintegrowane rozwiązanie do tworzenia kopii zapasowych dla serwerów fizycznych z systemem Windows/Linus, komputerów z systemem Windows, serwerów plików rsync/SMB oraz maszyn wirtualnych VMware vSphere/Microsoft Hyper-V
-Centralny interfejs zarządzania służący do monitorowania stanu wszystkich zadań tworzenia kopii zapasowych, zużycia pamięci masowej i transmisji danych historycznych
-Różne metody przywracania, w tym przywracanie całego urządzenia, natychmiastowe przywracanie, szczegółowe odzyskiwanie plików
-Maksymalna wydajność tworzenia kopii zapasowych i pamięci masowej dzięki zastosowaniu funkcji Changed Block Tracking (CBT), narzędzia RCT (Resident Change Tracking) oraz deduplikacji globalnej
-Elastyczne zasady planowania i przechowywania w celu dostosowywania strategii tworzenia kopii zapasowych
-Szczegółowe logi i raporty umożliwiające śledzenie stanów kopii zapasowych i diagnostykę problemów

Komputer osobisty (Windows)
-Obsługiwane platformy: Windows 10 Creators Update (wszystkie wersje), Windows 10 (wszystkie wersje), Windows 8.1 (wszystkie wersje) i Windows 7 SP1 (wszystkie wersje)
-Obsługa systemu plików NTFS
-Tryby tworzenia kopii zapasowej: Kopia zapasowa całego urządzenia, wolumenu systemowego i niestandardowego wolumenu
-Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów oraz przywracanie na poziomie woluminów
-Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym danych i konfiguracji systemu
-Kopia zapasowa oparta na agencie tworzy kopie zapasowe i przywraca zmienione bloki znalezione między migawkami

-Korzystanie z funkcji śledzenia zmiany bloków Changed Block Tracking opartej na usłudze Microsoft VSS do tworzenia przyrostowych kopii zapasowych
-Zdarzenia tworzenia kopii zapasowych wyzwalane zdarzeniami obejmują blokadę ekranu urządzenia, wylogowanie użytkownika i uruchamianie urządzeń
-Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowej
-Systemem plików w miejscu docelowym kopii zapasowej musi być Btrfs
-Obsługa tworzenia kopii zapasowych tylko na zewnętrznych dyskach twardych. Inne urządzenia zewnętrzne, takie jak dyskietki, napędy USB i czytniki kart pamięci flash nie są obsługiwane

Serwer fizyczny (Windows)
Dane techniczne

-Obsługiwane platformy: Windows 10 Creators Update (wszystkie wersje), Windows 10 (wszystkie wersje), Windows 8.1 (wszystkie wersje), Windows 7 SP1 (wszystkie wersje), Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 i Windows Server 2019
-Obsługa systemu plików NTFS
-Tryby tworzenia kopii zapasowych: Kopia zapasowa całego urządzenia, wolumenu systemowego i niestandardowego wolumenu
-Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów, przywracanie na poziomie woluminów i natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V lub równoznacznego oprogramowania
-Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym danych i konfiguracji systemu
-Kopia zapasowa oparta na agencie tworzy kopie zapasowe zmienionych bloków znalezionych między migawkami
-Korzystanie z funkcji do śledzenia zmiany bloków Changed Block Tracking w oparciu o usługę Microsoft VSS w celu wykonywania przyrostowych kopii zapasowych
-Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowej
-Systemem plików w miejscu docelowym kopii zapasowej musi być Btrfs
-Obsługa tworzenia kopii zapasowych tylko na zewnętrznych dyskach twardych. Inne urządzenia zewnętrzne, takie jak dyskietki, napędy USB i czytniki kart pamięci flash nie są obsługiwane
-W przypadku tworzenia kopii zapasowych dysków dynamicznych obsługiwane są tylko woluminy proste, natomiast inne typy woluminów nie są obsługiwane

Serwer plików (SMB)
Dane techniczne

-Obsługiwany protokół SMB: SMB1, SMB2 i SMB3
-Tworzenie kopii zapasowych bez agentów
-ryby tworzenia kopii zapasowych: Wiele wersji, kopia lustrzana i przyrostowe kopie zapasowe
-Metoda przywracania: Przywracanie na poziomie plików/folderów

-Obsługa tworzenia kopii zapasowych listy ACL systemu Windows
-Obsługa usługi Windows VSS w celu zapewnienia spójności danych kopii zapasowej
-Jednoczesne wykonywanie zadań kopii zapasowej
-Systemem plików w miejscu docelowym kopii zapasowej musi być system Btrfs lub ext4

Maszyna wirtualna
Dane techniczne

-Obsługiwane platformy VMware vSphere: VMware vSphere 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 i 7.0.0
-Obsługiwane wersje VMware vSphere: VMware free ESXi, VMware vSphere Essentials, VMware vSphere Essentials Plus, VMware vSphere Standard, VMware vSphere Advanced, VMware vSphere Enterprise i VMware vSphere Enterprise Plus
-Obsługa wszystkich typów i wersji sprzętu wirtualnego VMware, w tym 62 TB VMDK
-Obsługiwane monitory maszyny wirtualnej Microsoft Hyper-V: Hyper-V 2016 i 2019
-Obsługa maszyn wirtualnych Hyper-V generacji 1 i 2, w tym dysków VHDX o pojemności 64 TB i wersji sprzętu wirtualnego od 5.0 do 9.0
-Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym konfiguracji danych i systemu
-Kopia zapasowa bez agentów
-Korzystanie z funkcji VMware Changed Block Tracking i funkcji Hyper-V Resilient Change Tracking do wykonywania przyrostowej kopii zapasowej
-Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowych
-Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów i natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V lub równorzędnego oprogramowania
-W przypadku przywracania na poziomie plików w systemie operacyjnym gościa obsługiwane systemy plików systemu Windows to NTFS i FAT32, a obsługiwane systemy plików systemu Linux to NTFS, FAT32, ext3, I ext4
-Kopia zapasowa uwzględniające aplikacje dla maszyn wirtualnych VMware vSphere lub Microsoft Hyper-V działających w systemie Microsoft Windows 2003 SP1 lub nowszym (z wyjątkiem Nano Server z powodu braku architektury VSS)
-Obsługa tworzenia kopii zapasowych systemów operacyjnych i aplikacji obsługiwanych przez rozwiązania VMware vSphere i Microsoft Hyper-V
-Systemem plików w miejscu docelowym kopii zapasowej musi być Btrfs

Portal przywracania
-Przywracanie pojedynczego pliku/folderu w celu zaoszczędzenia czasu przywracania
-Wyszukiwanie słów kluczowych użytkowników w celu łatwego znalezienia żądanych danych

Przywracanie danych
-Wzorzec wsadowy przywracania plików/folderów w tym samym katalogu
-Możliwość przywracania kopii zapasowych danych serwerów fizycznych z systemem Windows, serwerów plików i maszyn wirtualnych należących do częściowo pomyślnie przywróconych wersji

-Możliwość przywracania metadanych plików/folderów, takich jak czas modyfikacji, czas utworzenia i uprawnienia ACL podczas przywracania komputerów z systemem Windows oraz serwerów fizycznych i maszyn wirtualnych z systemem Windows/Linux
-Pobieranie wsadowe plików/folderów w tym samym katalogu
-Plik/folder pobrany wsadowo zostanie skompresowany do pojedynczego pliku
-Możliwość pobrania kopii zapasowej serwerów fizycznych z systemem Windows, serwerów plików i maszyn wirtualnych należących do częściowo pomyślnie przywróconych wersji

Dysk – zamontowane 3 sztuki

- Pobór mocy (zapis): maks 10 W
- Waga produktu: maks 1 kg
- Zakres temperatur (przechowywanie): -40 - 70 °C
- Rozmiar HDD: 3.5"
- Limit obciążenia pracą: min. 180 TB/rok
- Poziom szumu, bezczynny: maks 40 dB
- Pobór mocy (odczyt): maks. 10 W
- Pobór mocy w trybie czuwania: maks. 0,5 W
- Standardowe rozwiązania komunikacyjne: Serial ATA III
- Pobór mocy (bezczynny): maks. 5 W
- Szybkość transmisji interfejsu HDD: 6 Gbit/s
- Wstrząsy podczas przechowywania: 250 G
- Zakres temperatur (eksploatacja): 0 - 65 °C
- Pojemność HDD: min. 10000 GB
- Szybkość HDD: min. 7200 RPM
- Nominalny czas pracy: min. 1 mln godzin
- Gwarancja sprzedawcy/producenta : min. 36 miesięcy

Część IV: Modernizacja sieci, Access point

Modernizacja sieci teleinformatycznej

STAN ISTNIEJĄCY

Główna siedziba Urzędu Gminy w Paprotni mieści się w piętrowym budynku pod adresem ul. 3 Maja 2, 08-107 Paprotnia.
Obecnie Zamawiający dysponuje siecią komputerową wykonana ponad 10 lat temu. Sieć posiada topologię gwiazdy z głównym punktem dystrybucyjnym sieci LAN umiejscowionym w serwerowni w pomieszczeniu na piętrze. Łączność z punktami dystrybucyjnymi realizowana jest z wykorzystaniem skrętki miedzianej. Okablowanie pionowe sieci wykonane jest w oparciu o skrętkę UTP kategorii 5e.
Z uwagi na brak wolnych gniazd abonenckich, występują połączenia łańcuchowe, w których

wykorzystywane są niezarządzalne przełączniki rozdzielające sygnał dla użytkowników bezpośrednio w pokojach.
Sieć komputerowa nie posiada dedykowanego zasilania elektrycznego. Całość sprzętu informatycznego podpięta jest do zasilania ogólnego wspólnego dla innych odbiorników. Stanowiska komputerowe wyposażone są w urządzenia ochrony przeciwprzepięciowej (UPS). To samo dotyczy punktu dystrybucyjnego.

ZAKRES USŁUG

Przedmiotem zapytania ofertowego jest modernizacja sieci teleinformatycznej polegająca na:

1. Dodaniu gniazd RJ-45, listw kablowych naściennych, zarobieniu przewodów we wszystkich nowych punktach oraz w patchpanelu (również skrosowanie od nowa 20 „starych" przewodów), montaż nowego Access Pointa oraz położenie nowych przewodów od punktu dystrybucyjnego do gniazd w poszczególnych pomieszczeniach.
2. Wykonanie dokumentacji architektury sieci teletechnicznej (schemat fizyczny 2D) po modernizacji.
   Zestawienie materiałów niezbędnych przy modernizacji instalacji:

LP.	**Sieć teleinformatyczna**	**ILOŚĆ**
1.	Gniazda RJ-45 podwójne kategorii 5e	4 szt.
2.	Skrętka komputerowa UTP kat. 5e	112 m.b.
4.	Listwa naścienna 25x16	35 m.b.
5.	Patch panel 24 port kat. 5e	1 szt
6.	Patchcord kat. 5e 0,5m	24 szt.

Zastosowane gniazda logiczne RJ-45 powinny być nierozłączne, tj. w jednym module złącze terminacji kabla i część gniazda RJ45 (bez wymiennych wkładek wprowadzających dodatkowe złącze w gnieździe).
Wiązka kabli miedzianych UTP kat. 5e ma być rozszyta na patchpanelu zamontowanym w szafie dystrybucyjnej na piętrze budynku (w serwerowni).

Wszelkie uzasadnione zmiany, które wykonawca chciałby wprowadzić do przedmiotu zamówienia (na etapie wykonawstwa) muszą być uzgodnione zamawiającym. Wszelkie prace -montażowe związane z realizacją niniejszego zadania należy wykonać zgodnie z obowiązującymi normami oraz wytycznymi technicznymi, a w szczególności przestrzegać przepisów BHP. Wszystkie wykonywane prace oraz proponowane materiały winny odpowiadać Polskim Normom i posiadać stosowną deklarację zgodności lub posiadać znak CE i deklarację zgodności z normami zharmonizowanymi oraz posiadać niezbędne atesty tak aby spełniać obowiązujące przepisy.

Zaleca się wykonać wizję lokalną na obiekcie przed złożeniem oferty w celu zapoznania się ze strukturą budynku w celu poprawnego oszacowania nakładów na pracę i możliwości zastosowania rozwiązań technicznych.

Wykonawcy ubiegający się o udzielenie niniejszego zamówienia muszą dysponować odpowiednim potencjałem technicznym, wiedzą i doświadczeniem oraz osobami zdolnymi do wykonania zamówienia. Wykonawca dołączy do oferty kserokopię uprawnień elektrycznych SEP do 1kV osoby wyznaczonej do wykonania przedmiotu zamówienia. Wykonawca usługi zobowiązany jest udzielić na wykonany przedmiot zamówienia co najmniej 24 miesiące gwarancji, licząc od dnia podpisania protokołu odbioru usługi bez uwag.

Access point

Interfejs sieciowy: min. 2 gigabitowe porty Ethernet 10/100/1000

- **Liczba portów USB 2.0:** min. 1
- **Antena:** min. **3** anteny
- **Standardy WiFi:** 802.11 a/b/g/n/ac
- **Sposób zasilania:** Pasywne PoE 24 V (pairs 4, 5+; 7, 8 Return) lub PoE 802.3af/A 48 V
- **Maksymalny pobór mocy:** 10 W
- **Minimalny zakres wewnętrzny (pomieszczenie):** 120m
- **Minimalna moc TX:** 2,4 GHz: 20 dBm 5 GHz: 20 dBm
- **Minimalny transfer danych przez bezprzewody LAN:** 1200 Mb/s
- **BSSID:** min. 4
- **Oszczędzanie energii:** Wspierane
- **Zabezpieczenia transmisji bezprzewodowej:** WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
- **Certyfikaty:** CE, FCC, IC
- **Montaż:** Na ścienia lub suficie (uchwyty w zestawie)
- **Dopuszczalna temperatura pracy:** Od -10 do 70 st. C
- **Dopuszczalna wilgotność powietrza:** 5%-95% niekondensująca
- **VLAN:** 802.1Q
- **Zaawansowane QoS:** Limitowanie przepustowości na użytkownika
- **Guest Traffic Isolation:** Wspierane
- **WMM:** Voice, video, best effort, background
- **Liczba klientów podłączonych jednocześnie:** min. 100