**Załącznik nr 6**

**Szczegółowy opis przedmiotu zamówienia**

**Zadanie nr 1 Dostawa urządzeń sieciowych oraz backup**

1. ***Dostawa urządzenia UTM – 1 sztuka***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, typ, model)*

# **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.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

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.

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

System musi wspierać IPv4 oraz IPv6 w zakresie:

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

# **Redundancja, monitoring i wykrywanie awarii**

1. 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.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

# **Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:

* 16 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 2 gniazdami SFP+ 10 Gbps.

1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w **redundantne** zasilanie AC.

# **Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz **56** tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 64 B.
4. Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 1518 B.
5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż **2.2** Gbps.
6. Wydajność szyfrowania IPSec VPN nie mniej niż **11.5** Gbps.
7. 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 **2.6** Gbps.
8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

# **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:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. 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.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Analiza ruchu szyfrowanego protokołem SSH.
13. 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**

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. 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.

1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
3. 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
* Cisco ACI.
* Google Cloud Platform (GCP).
* Nuage Networks VSP.
* OpenStack.
* VMware vCenter (ESXi).
* VMware NSX.

·       VMware NSX.Nutanix

·       VMware NSX.IBM Cloud

# **Połączenia VPN**

1. 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.

1. 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.
3. Rozwiązanie powinno wspierać funkcję Forward Error Correctionm na tunelach IPSec.
4. Funkcja monitorowania łącza w oparciu o rzeczywisty ruch bez konieczności tworzenia dedykowanych detektorów.

# **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 (co najmniej: Facebook, Google Docs, Dropbox) 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. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
9. Filtrowanie treści wideo w oparciu o kategorie - co najmniej dla servisów youtube, vimeo.
10. Blokowanie wysyłania poświadczeń firmowych do obcych serwisów.

# **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.

1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
3. 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. 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.
2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
3. Musi istnieć możliwość logowania do serwera SYSLOG.

# **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:

a)     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 **36** miesięcy.

# **Gwarancja oraz wsparcie**

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres **36** 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.

# **Rozszerzone wsparcie serwisowe**

a)       System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres **36** miesięcy.

c)       Dla zapewnienia wysokiego poziomu usług oferent musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy **lub adres emailowy** oraz infolinię w języku polskim 8x5

d)       **Dla zapewnienia wysokiego poziomu usług oferent musi wykazać, iż dysponuje minimum dwoma certyfikowanymi inżynierami z oferowanej technologii: jeden z najwyższym możliwym certyfikatem technicznym, drugi z certyfikatem o jeden stopień niższym. W tym celu do oferty należy załączyć ww. certyfikaty.**

**e) Zamawiający wymaga przeniesienia konfiguracji z posiadanego przez siebie urządzenia FortiGate60d na nowe urządzenie oraz wdrożenia nowego urządzenia w sieci produkcyjnej Zamawiającego.**

**f) Zamawiający wymaga dodatkowej opieki powdrożeniowej w lokalizacji Zamawiającego w ilości 48h przez okres 6 miesięcy od wdrożenia.**

* Oświadczanie Producenta lub Autoryzowanego Dystrybutora lub Partnera świadczącego wsparcie techniczne  o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu **lub adres emailowy** i numer infolinii telefonicznej).
* Certyfikat ISO 9001 podmiotu serwisującego.

1. ***Dostawa Autoloadera taśmowego SAS - 1 sztuka***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, typ, model)*

1. Autoloader taśmowy musi być wyposażony w jeden napęd LTO Ultrium-8 SAS o wydajności natywnej co najmniej 1TB/h oraz pojemności pojedynczej taśmy co najmniej 12TB – parametry podane bez kompresji danych.

2. Oferowany autoloader musi być wyposażony w co najmniej 8 slotów na taśmy magnetyczne.

3. Oferowany napęd taśmowy musi być wyposażony w mechanizm dostosowujący automatycznie oraz płynnie prędkość przesuwu taśmy magnetycznej do wartości strumienia danych przekazywanego do napędu w zakresie co najmniej 101-300MB/s.

4. Wysokość oferowanego autoloadera taśmowego nie może przekraczać 1U. Wraz z urządzeniem należy dostarczyć odpowiedni zestaw montażowy do szafy 19”.

5. Oferowany autoloader taśmowy musi posiadać możliwość zdalnego zarządzania za pośrednictwem przeglądarki internetowej.

6. Oferowany autoloader musi być wyposażony w czytnik kodów kreskowych.

7. Wraz z autoloaderem należy dostarczyć 8 szt. taśm LTO-8 RW wraz z etykietami oraz 1 szt. taśmy czyszczącej.

8. Oferowany autoloader musi być przystosowana do montażu w szafie 19”.

9. Oferowana autoloader taśmowy musi posiadać możliwość konfiguracji co najmniej jednego tzw. „mail slot” umożliwiającego wymianę pojedynczej taśmy bez konieczności wyjmowania z biblioteki całego magazynka z taśmami.

10. Dla oferowanego autoloadera taśmowego parametr MTBF musi wynosić co najmniej 100 000 godzin.

11. Dla oferowanego autoloadera taśmowego parametr MSBF musi wynosić co najmniej 2 000 000 pełnych cykli „załaduj/wyładuj”.

12. Oferowany autoloader powinien posiadac port USB w który można w przyszłości dołączyć pamięć USB zawierającą klucze szyfrujące dane zapisywane w napędzie.

13. Minimum 3-letnia gwarancja producenta w miejscu instalacji świadczona w trybie 8x5. Gwarantowany czas reakcji serwisu na następny dzień roboczy (NBD) realizowany przez polski oddział serwisu producenta posiadającego certyfikat ISO.

1. ***Dostawa przełącznika sieciowego zarządzalnego – 1 sztuka***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, typ, model)*

* 1. Urządzenie musi być wyposażone w minimum 24 porty 10 Gigabit Ethernet SFP+ oraz minimum 6 portów 40 Gigabit Ethernet QSFP28.
  2. Urządzenie musi być dostarczone z zainstalowanymi we wszystkich portach 10Gb modułami SFP+ typu MultiMode ze złączem LC Wkładki SFP+ muszą być oryginalne i pochodzić od producenta przełącznika celem uniknięcia problemów z serwisowaniem urządzenia.
  3. Urządzenie musi umożliwiać stworzenie wirtualnego systemu - złożonego z min. 2 zarządzanego jako jedno urządzenie logiczne. Urządzenia pracujące w takiej konfiguracji muszą umożliwiać połączenie w system z wykorzystaniem standardowych portów 10Gigabit Ethernet / 40 Gigabit Ethernet / 1000 Gigabit Ethernet oraz modułów optycznych lub kabli DAC. Musi istnieć możliwość terminowania połączeń link aggregation na dwóch przełącznikach tworzących taki system wirtualny (tzw. multi-chassis link aggregation)
  4. Urządzenie musi być wyposażone w wewnętrzny zasilacz 230V AC wspierający mechanizm HotSwap z możliwością instalacji drugiego zasilacza do pracy w trybie redundantym.
  5. Urządzenie musi być wyposażone w wewnętrzne wentylatory zapewniające chłodzenie urządzenia.
  6. Wymagane parametry wydajnościowe:
* Switching capacity: minimum 1,6 Tbps
* Forwarding capacity: minimum 410 Mpps
* min. 81 000 wpisów w tablicy adresów MAC
* min. 100 000 wpisów w tablicy ARP
* min. 80 000 wpisów w tablicy routingowej IPv4
* min. 80 000 wpisów w tablicy routingowej IPv6
* min. 30 000 tras multicast
* min. 6 000 wpisów na potrzeby realizacji polityk bezpieczeństwa (listy kontroli dostępu ACL)
* min. 1 000 interfejsów VLAN
* min. 3900 aktywnych sieci VLAN
  1. Urządzenie musi posiadać obsługę protokołów warstwy 3 dla IPv4: Open Shortest Path First (OSPF), BGPv4, ISIS-IPv4
  2. Urządzenie musi posiadać obsługę protokołów warstwy 3 dla IPv6: Open Shortest Path First (OSPFv3), BGP+, ISIS-IPv6
  3. Urządzenie musi posiadać obsługę protokołów multicastowych w tym PIM Sparse i Dense Mode, SSM, IGMP/MLD
  4. Urządzenie musi posiadać obsługę protokołów MPLS, LDP, L2 i L3 VPN, VPLS, MPLS TE, MPLS.
  5. Urządzenie musi umożliwiać rozbudowę o funkcjonalność VxLAN w przyszłości poprzez np.: zakup licencji,
  6. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
* mechanizm BFD (Bidirectional Forwarding Detection) co najmniej dla protokołu OSPFv2 i OSPFv3, BGP, ISIS
* IEEE 802.1w Rapid Spanning Tree
* IEEE 802.1s Multiple Spanning Tree
* IEEE 802.3ad (Link Aggregation Control Protocol) umożliwiający grupowanie portów.  
  1. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci (QoS):
* Obsługa min. 8 kolejek per port, w tym co najmniej jedna kolejka ze statusem strict priority
* Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez nadawanie wartości 802.1p (CoS) oraz IP Precedence/DSCP w ramkach Ethernet oraz pakietach IP. Wykorzystanie następujących parametrów w klasyfikacji: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, żródłowy/docelowy port TCP
* Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet oraz pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP Precedence/DSCP
* Definiowanie polityk QoS per port i per VLAN  
  1. Urządzenie musi wspierać następujące mechanizmy związane z bezpieczeństwem:
* Wiele poziomów dostępu administracyjnego poprzez konsolę - autoryzacja dostępu do przełącznika w oparciu o mechanizmy AAA – min. 5 poziomów uprawnień z możliwością określenia zakresu z dokładnością do poszczególnych komend
* Autoryzacja użytkowników/portów w oparciu o IEEE 802.1X z możliwością przydziału listy kontroli dostępu (ACL) i VLANu
* Obsługa co najmniej następujących mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard
* Weryfikacja źródła pakietu względem tablicy routingu (uRPF) – zarówno dla IPv4 i IPv6
* Możliwość filtrowania ruchu na poziomie portu oraz VLANu w oparciu o adresy MAC, IP, porty TCP/UDP
* Listy kontroli dostępu także dla IPv6
* Mechanizmy ochrony warstwy kontrolnej  
  1. Urządzenie musi posiadać obsługę ramki Ethernet o wielkości nie mniejszej niż 9216 bajtów (tzw. Jumbo Frame)
  2. Urządzenie musi być przystosowane do montażu w szafie 19”, wysokość nie większa niż 1RU, elementy niezbędne do montażu muszą być dostarczone z urządzeniem
* Urządzenie musi wspierać następujące mechanizmy związane z zarządzaniem:
* Ma możliwość zarządzania przez WEB Gui (HTTPS), SNMPv3 oraz SSH v2
* Umożliwia zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Ethernet out-of-band management
* Umożliwia identyfikację i uwierzytelnianie w oparciu o serwer RADIUS lub TACACS+
* Posiada port USB
* Umożliwia lokalną/zdalną obserwację ruchu na określonym porcie (SPAN,RSPAN), polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez dedykowaną sieć VLAN
* Posiada możliwość raportowania do systemów zarządzających z wykorzystaniem statystyk typu flow (J-Flow, NetFlow, sFlow lub odpowiednik).
* Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych  
  1. Urządzenie musi być wyposażone w zintegrowany kontroler sieci WLAN zdolny do pracy w klastrze HA przy utworzeniu stosu przełączników o parametrach wskazanych w pkt 1.19-1.54.
  2. W ramach rozwiązania równoważnego dopuszcza się dostarczenie osobnego kontrolera WLAN z możliwością pracy w klastrze HA spełniającego parametry wskazane w pkt 1.19-1.54.
  3. Wymagane Parametry kontrolera sieci WLAN
  4. Kontroler sieci bezprzewodowej wyposażony w licencję która umożliwia centralne zarządzanie minimum 15 bezprzewodowymi punktami dostępowymi(AP) z możliwością rozbudowy poprzez dokupienie licencji aby objąć zarządzaniem minimum 150 bezprzewodowych punktów dostępowych.
  5. Kontroler WLAN musi umożliwiać zarządzanie punktami dostępowymi znajdowującymi się w tej samej domenie rozgłoszeniowej oraz znajdującymi się w innej podsieci IP
  6. Kontroler musi obsługiwać możliwość łączenia kontrolerów w grupy urządzeń w celu zapewnienia redundancji (wymagane tryby 1+1 oraz N+1)
  7. Podłączanie bezprzewodowych punktów dostępowych poprzez warstwę 2 i 3
  8. Minimum 3000 obsługiwanych użytkowników
  9. Minimum 48 obsługiwanych grup użytkowników
  10. Obsługa co najmniej 1000 list kontroli dostępu (ACL). Obsługa list ACL opartych o adresy MAC (źródłowy i docelowy), adresy IP (źródłowy i docelowy), typ protokołu, port (TCP i UDP) a także grupę użytkowników
  11. Funkcja działania list ACL w określonych przedziałach czasu
  12. Uwierzytelnianie oparte o adresy MAC, 802.1x (co najmniej EAP-PAP, EAP-MD5, EAP-PEAP, EAP-TLS, EAP-TTLS), zewnętrzny portal WWW (Captive Portal), wbudowany portal WWW, oraz adres MAC i portal WWW
  13. Lokalna baza użytkowników obsługująca co najmniej 1000 wpisów (użytkowników).
  14. Funkcja automatycznego przekierowywania na 5GHz klientów obsługujących tą częstotliwość.
  15. Zgodność ze standardem IETF 5415 CAPWAP
  16. Zgodność z 802.11a,802.11b,802.11g,802.11n,802.11e,802.11d,11ac,11ax(WiFi 6.0)
  17. Automatyczne i ręczne wybieranie kanałów oraz mocy nadawczej
  18. Wbudowany serwer DHCP obsługujący co najmniej 64 pule adresów IP
  19. Obsługa funkcji DHCP klient i DHCP relay
  20. Obsługa funkcji: ochrony serwera DHCP, DHCP snooping, Dynamic ARP Inspection, IP Source Guard
  21. Obsługa IEEE 802.1s Multiple SpanningTree (MSTP) oraz IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
  22. Obsługa 802.3ad Link Aggregation Protocol (LACP)
  23. Funkcja BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom
  24. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
  25. Obsługa routingu statycznego i dynamicznego (co najmniej protokoły: RIP, OSFP, ISIS, BGP)
  26. Obsługa routingu bazującego na politykach (Policy Based Routing)
  27. Obsługa IGMP v1/v2/v3 oraz IGMP snooping i IGMP proxy
  28. Obsługa protokołu PIM-SM
  29. Funkcja izolacji użytkowników radiowych (wewnątrz grupy a także pomiędzy grupami użytkowników)
  30. Funkcja automatycznego zwiększa mocy pobliskich AP w przypadku awarii jednego z nich w celu zapewnienia pełnego pokrycia sygnałem WiFi
  31. Obsługa sieci IEEE 802.1Q VLAN – minimum 4 000 sieci VLAN obsługiwanych równocześnie
  32. Zarządzanie poprzez wbudowane Web GUI jak i możliwe zarządzanie przy pomocy zewnętrznego serwera z Web GUI
  33. Zarządzanie poprzez port konsoli (CLI)
  34. Wsparcie dla SNMP v1/v2/v3
  35. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
  36. Obsługa trybu przełączania centralnego (ruch z klienta radiowego tunelowany do kontrolera), trybu rozproszonego (ruch z klienta radiowego mapowany bezpośrednio z AP do sieci VLAN) oraz trybu hybrydowego (przełączanie centralne przed autentykacją klienta i rozproszone po autentykacji). Wybór trybu pracy musi być możliwy co najmniej per punkt dostępowy i per SSID
  37. Kontroler musi zapewniać równomierne rozmieszczenie klientów radiowych na poszczególnych punktach dostępowych tzw. load balancing. Musi być on realizowany bazując na liczbie klientów oraz obciążeniu
  38. Funkcja analizy spectrum. Identyfikacja źródeł zakłóceń pochodzących od: Bluetooth, kuchenki mikrofalowej, telefonów bezprzewodowych, ZigBee, innych urządzeń wykorzystujących pasma bliskie 2.4 GHz i 5 GHz
  39. Wymagany jest gwarancja w trybie Lifetime tj nie krótsza niż 5 lat od daty zakończenia sprzedaży oferowanego modelu.
  40. Możliwość zgłaszania problemów w trybie 8x5 z czasem reakcji następnego dnia roboczego .
  41. Rozwiązywanie problemów ze sprzętem i oprogramowaniem.
  42. W przypadku konieczności wymiany na nowe urządzenie zostanie ono dostarczone maksymalnie w ciągu 14 dni od momentu zgłoszenia
  43. Dostęp do poprawek i nowych wersji oprogramowania
  44. Ze względów ujednolicenia i uproszczenia procedur gwarancyjnych wymaga się aby przełącznik był tego samego producenta co z pozycji nr 4.

1. ***Dostawa switchy zarządzalnych - 4 sztuki***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, typ, model)*

|  |  |
| --- | --- |
| Element | Charakterystyka |
| Minimalne wymagania sprzętowe: | * Urządzenie fabrycznie nowe, nieużywane * Obudowa przeznaczona do montażu w szafie 19”. Wysokość obudowy nie większa niż 1 RU. * Obudowa musi być wykonana z metalu. Ze względu na różne warunki, w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowanie plastikowej. * Urządzenie musi być przystosowane do pracy w temperaturze otoczenia od 5 do 45 stopni Celsjusza. * minimum 4 porty 10GE SFP+ . Urządzenie musi być dostarczone z zainstalowanymi we wszystkich portach 10Gb modułami SFP+ typu MultiMode ze złączem LC Wkładki SFP+ muszą być oryginalne i pochodzić od producenta przełącznika celem uniknięcia problemów z serwisowaniem urządzenia. * minimum 48 portów Ethernet 1000BaseT (Rj45) z auto-negocjacją 10/100/1000 z obsługą Power over Ethernet w standardzie 802.3af i 802.3at * Budżet mocy dla funkcji PoE minimum 870W. * Wymagane jest aby wszystkie powyższe porty mogły działać jednocześnie. * Wydajność przełącznika min. 176 Gb/s i min. 130 Mpps * Przełącznik wyposażony w wymienny zasilacz 230V/AC. * Urządzenie musi mieć możliwość łączenia przełączników fizycznych w jeden przełącznik wirtualny, traktowany jako jedno urządzenie logiczne z punktu widzenia protokołów routingu, LACP i Spanning Tree. * Minimalna liczba przełączników obsługiwanych w stosie 9szt. * Funkcja tworzenia stosu może wykorzystywać maksymalnie dwa wbudowane porty 10GE SFP+ lub dedykowany moduł który musi zostać zainstalowany w takim przypadku wraz z niezbędnym okablowaniem. * Przełączanie w warstwie drugiej i trzeciej modeli ISO/OSI. * Port konsoli * Minimum jeden port USB obsługujący pamięci masowe typu Pendrive |
| Funkcje warstwy 2 | * GARP VLAN Registration Protocol (GVRP) * Rozmiar tablicy MAC minimum 16 000 adresów * 4000 aktywnych sieci VLAN * Mapowanie VLAN-ów 1:1 * Agregacja portów statyczna i przy pomocy protokołu LACP * Min. 20 grup portów zagregowanych, możliwość stworzenia grupy z min. 8 portów, również między przełącznikami pracującymi w stosie. * Spanning Tree: MSTP 802.1s, RSTP 802.1w, STP Root Guard * Protokół umożliwiający tworzenie szybkobieżnych sieci w topologii pierścieni w których czas przełączenia transmisji na ścieżkę zapasową jest mniejszy niż 50ms np. ERPS lub równoważny. |
| Funkcje warstwy 3 | * Minimum 1000 interfejsów VLAN * routing IPv4 z prędkością łącza, * wsparcie dla routingu IPv4: statycznego , RIP, OSPF * routing IPv6 z prędkością łącza, * wsparcie dla routingu IPv6: statycznego, RIPng, * Rozmiar tablicy routingu 4 000 wpisów IPv4 oraz 1000 wpisów IPv6. * Virtual Router Redundancy Protocol (VRRP) * Policy-based routing * IGMP Snooping v1/v2/v3 |
| Bezpieczeństwo | * DHCP Snooping (wsparcie dla Option 82) * RADIUS * Secure Shell (SSHv2) * IEEE 802.1X– dynamiczne dostarczanie polityk QoS, ACLs i sieci VLANs: zezwalające na nadzór nad dostępem użytkownika do sieci * PORTAL Authentication * Guest VLAN * Private VLAN lub równoważny. * Port security: zezwalający na dostęp tylko specyficznym adresom MAC * MAC-based authentication * IP source guard * MFF(MAC Forced Forwarding) lub równoważny umożliwiający blokowanie ruchu tzw. poziomego w całej sieci LAN na wszystkich przełącznikach i wymuszanie komunikacji między hostami przez urządzenie typu L3 Gateway (np. router lub firewall) * Loopback Detection * Urządzenie musi być odporne na ataki typu Denial of service takich jak SYN Flood attacks, Land attacks, Smurf attacks, oraz ICMP Flood attacks |
| Quality of Service (QoS) | * Funkcje QoS: kreowanie klas ruchu w oparciu o access control lists (ACLs), IEEE 802.1p precedence, IP, DSCP oraz Type of Service (ToS) precedence; * 8 kolejek QoS per port |
| Monitoring i diagnostyka | * Port mirroring (SPAN) i Remote Port mirroring (RSPAN) * OAM (802.3ah) i CFM (802.1ag): wykrywanie problemów na łączu pomiędzy urządzeniami |
| Zarządzenie | * Zdalna konfiguracja i zarządzanie przez Web (https) oraz linię komend (CLI) * IEEE 802.1ab LLDP oraz LLDP-MED * Pamięć flash o pojemności pozwalającej na przechowywanie minium dwóch wersji oprogramowania systemowego * Serwisy DHCP: serwer (RFC 2131), klient i relay * SNMPv1, v2, v3 * Syslog |
| Serwis gwarancyjny | * Wymagany jest gwarancja w trybie Lifetime tj nie krótsza niż 5 lat od daty zakończenia sprzedaży oferowanego modelu. * Możliwość zgłaszania problemów w trybie 8x5 z czasem reakcji następnego dnia roboczego . * Rozwiązywanie problemów ze sprzętem i oprogramowaniem. * W przypadku konieczności wymiany na nowe urządzenie zostanie ono dostarczone maksymalnie w ciągu 14 dni od momentu zgłoszenia * Dostęp do poprawek i nowych wersji oprogramowania |
| Inne | * Ze względów ujednolicenia i uproszczenia procedur gwarancyjnych wymaga się aby przełącznik był tego samego producenta co z pozycji nr 3. |

1. ***Dostawa oprogramowania do backupu dla maszyny fizycznej – 1 sztuka***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, wersja)*

Zamawiający wymaga 1 licencji z minimum 5-cio letnią subskrypcją (aktualizacje wraz z supportem)

1. Produkt i dokumentacja dostępna w polskiej (i angielskiej) wersji językowej
2. Wsparcie dla systemów operacyjnych Windows typu serwer i stacja robocza:

***Systemy operacyjne Windows***: Windows Server 2016, 2012/2012 R2, 2008/2008 R2, 2003/2003 R2, Windows Small Business Server 2011, 2008, 2003/2003 R2, Windows MultiPoint Server 2012, 2011, 2010, Windows Storage Server 2012/2012 R2, 2008/2008 R2, 2003, Windows 10, 8.1, 8, 7, Vista, XP SP3

1. Wsparcie i pełna funkcjonalność oprogramowania dla wielojęzykowych systemów operacyjnych
2. Tworzenie kopii zapasowych dysków/partycji
3. Tworzenie kopii zapasowych plików i folderów
4. Replikacja kopii zapasowych do wielu lokalizacji docelowych
5. Tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
6. Kopie zapasowe i granularne przywracanie elementów aplikacji Microsoft Exchange, Microsoft SQL Server, Microsoft SharePoint i Microsoft Active Directory.
7. Możliwość przywrócenia kopii zapasowej dysku/partycji na innym komputerze o innej konfiguracji sprzętowej
8. Obsługa dysków twardych z sektorami o rozmiarze 4KB oraz dysków SSD
9. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
10. Zdalna instalacja i aktualizacja agentów na komputerach klienckich
11. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych oraz serwerach SFTP
12. Obsługa napędów taśmowych.
13. Deduplikacja kopii zapasowych.
14. Możliwość generowania planu przywracania kopii zapasowych
15. Możliwość eksportu i importu planów tworzenia kopii zapasowych na różnych maszynach
16. Szablony schematów rotacji kopii zapasowych
17. Polecenia poprzedzające/następujące
18. Automatyczne usuwanie nieaktualnych kopii zapasowych (retencja)
19. Sprawdzanie poprawności i konsolidacja kopii zapasowych (pełnych, przyrostowych i różnicowych)
20. Wykonywanie zadań i tworzenie kopii zapasowych możliwe z poziomu wiersza polecenia.
21. Możliwość utworzenia ukrytej partycji widzianej tylko przez oprogramowanie do backupu na potrzeby zapisu kopii zapasowych, która będzie chroniona za pomocą hasła
22. Współpraca z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
23. Pełne, przyrostowe i różnicowe kopie zapasowe
24. Wysyłanie powiadomień pocztą e-mail
25. Szyfrowane kopii zapasowych algorytmem AES
26. Tworzenie dynamicznych grup urządzeń na podstawie nazwy urządzenia, ilości pamięci operacyjnej, zakresu adresów IP, typu systemu operacyjnego
27. Możliwość wykonywania czynności przenoszenia kopii zapasowych, replikacji, weryfikacji i czyszczenia na innym systemie.

**Funkcjonalność unikalna:**

1. Funkcja aktywnej ochrony przed oprogramowaniem ransomware, chroniąca pliki lokalne i pliki kopii zapasowych przed zaszyfrowaniem.
2. Predefiniowany schemat tworzenia kopii zapasowych: G-F-S
3. Priorytetowe przywracanie systemu operacyjnego - Jeśli system uległ awarii, można go uruchomić w ciągu kilku sekund, a proces przywracania będzie wykonywany w tle.
4. Uruchamianie usług z minimalnymi prawami użytkownika
5. Zaawansowane raportowanie - możliwość tworzenia raportów w oparciu o predefiniowane schematy
6. Pomoc techniczna dostępna w języku polskim
7. Administrowanie kontami użytkowników Acronis i jednostkami organizacyjnymi
8. Tworzenie kryptograficznego odcisku pliku (sumy kontrolnej) wykorzystującego technologię blockchain

**Punkty rezerwowe:**

1. Wykonywanie kopii zapasowych uruchamiane po wystąpieniu określonych zdarzeń i warunków
2. Migawki wielowoluminowe
3. Kopia zapasowa „sektor po sektorze"
4. Obsługa dysków dynamicznych
5. Automatyczne ponawianie prób w przypadku niekrytycznych błędów (prób utworzenia kopii zapasowej)
6. Możliwość utworzenia nośnika startowego opartego na środowisku Linux lub WinPE
7. ***Dostawa oprogramowania do backupu dla maszyn wirtualnych – 3 sztuki***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, wersja)*

Zamawiający wymaga 3 licencji z minimum 5-cio letnią subskrypcją (aktualizacje wraz z supportem)

1. Produkt i dokumentacja dostępna w polskiej (i angielskiej) wersji językowej
2. Wsparcie dla środowisk wirtualizacji: Hyper-V, VMware vSphere, Citrix XenServer, Red Hat Virtualization, Linux KVM I Oracle VM Server
3. Wsparcie i pełna funkcjonalność oprogramowania dla wielojęzykowych systemów operacyjnych
4. Tworzenie kopii zapasowych dysków/partycji
5. Tworzenie kopii zapasowych plików i folderów
6. Replikacja kopii zapasowych do wielu lokalizacji docelowych
7. Tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
8. Możliwość tworzenia kopii zapasowych maszyn wirtualnych Hyper-V i Vmware w sposób bezagentowy (agent na hoście).
9. Kopie zapasowe aplikacji Microsoft Exchange, Microsoft SQL Server, Microsoft SharePoint oraz Microsoft Active Directory i granularne przywracanie ich elementów
10. Wsparcie dla klastrów MS SQL i MS Exchange.
11. Możliwość przywrócenia kopii zapasowej dysku/partycji na innym komputerze o innej konfiguracji sprzętowej
12. Przyrostowe przywracanie kopii zapasowych maszyn wirtualnych VMware i Hyper-V w oparciu o technologię CBT (changed block tracking)
13. Obsługa dysków twardych z sektorami o rozmiarze 4KB oraz dysków SSD
14. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
15. Zdalna instalacja i aktualizacja agentów na hostach
16. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych oraz serwerach SFTP
17. Obsługa napędów taśmowych.
18. Deduplikacja kopii zapasowych.
19. Możliwość generowania planu przywracania kopii zapasowych
20. Możliwość eksportu i importu planów tworzenia kopii zapasowych na różnych maszynach
21. Szablony schematów rotacji kopii zapasowych
22. Polecenia poprzedzające/następujące
23. Automatyczne usuwanie nieaktualnych kopii zapasowych (retencja)
24. Sprawdzanie poprawności i konsolidacja kopii zapasowych (pełnych, przyrostowych i różnicowych)
25. Wykonywanie zadań i tworzenie kopii zapasowych możliwe z poziomu wiersza polecenia.
26. Możliwość utworzenia ukrytej partycji widzianej tylko przez oprogramowanie do backupu na potrzeby zapisu kopii zapasowych, która będzie chroniona za pomocą hasła
27. Współpraca z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
28. Pełne, przyrostowe i różnicowe kopie zapasowe
29. Wysyłanie powiadomień pocztą e-mail
30. Szyfrowane kopii zapasowych algorytmem AES
31. Tworzenie dynamicznych grup urządzeń na podstawie nazwy urządzenia, ilości pamięci operacyjnej, zakresu adresów IP, typu systemu operacyjnego
32. Możliwość wykonywania czynności przenoszenia kopii zapasowych, replikacji, weryfikacji i czyszczenia na innym systemie.

**Funkcjonalność unikalna:**

1. Funkcja aktywnej ochrony przed oprogramowaniem ransomware, chroniąca pliki lokalne i pliki kopii zapasowych przed zaszyfrowaniem.
2. Predefiniowany schemat tworzenia kopii zapasowych: G-F-S
3. Priorytetowe przywracanie systemu operacyjnego - Jeśli system uległ awarii, można go uruchomić w ciągu kilku sekund, a proces przywracania będzie wykonywany w tle.
4. Uruchamianie usług z minimalnymi prawami użytkownika
5. Zaawansowane raportowanie - możliwość tworzenia raportów w oparciu o predefiniowane schematy
6. Pomoc techniczna dostępna w języku polskim
7. Administrowanie kontami użytkowników Acronis i jednostkami organizacyjnymi
8. Tworzenie kryptograficznego odcisku pliku (sumy kontrolnej) wykorzystującego technologię blockchain

**Punkty rezerwowe:**

1. Wykonywanie kopii zapasowych uruchamiane po wystąpieniu określonych zdarzeń i warunków
2. Migawki wielowoluminowe
3. Kopia zapasowa „sektor po sektorze"
4. Obsługa dysków dynamicznych
5. Automatyczne ponawianie prób w przypadku niekrytycznych błędów (prób utworzenia kopii zapasowej)
6. Możliwość utworzenia nośnika startowego opartego na środowisku Linux lub WinPE

**Zadanie nr 2 Dostawa komputerów, monitorów, dysków, telefonów, akumulatorów, licencji oraz innych modułów**

1. ***Dostawa komputerów stacjonarnych – 14 sztuk***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, typ, model)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Poz.** | **Nazwa podzespołu** | **Wymagane parametry** | **TAK/NIE\***  **Oferowane parametry\*\*** |
| 1 | Procesor | Procesor wielordzeniowy, min. 6 rdzeni fizycznych  Minimum—13.200 punktów osiągniętych w teście PassMark CPU Mark  <https://www.cpubenchmark.net/cpu_list.php>  Układ musi pracować z fabrycznymi ustawieniami producenta (niedozwolony tzw. „overlock-ing”) | Producent procesora: …………………………….  Model procesora: …………..….…………………  Częstotliwość procesora: …….………………….  Wynik w testach: …………………………….. |
| 2 | Płyta główna | - Możliwość montażu dysku SATA  - BIOS pozwalający na oddzielne założenie hasła administratora i użytkownika | TAK/NIE |
| 3 | Pamięć operacyjna | Min. 16 GB  Możliwość rozbudowy do min. 64 GB | Ilość pamięci ……………………….  Możliwość rozbudowy do ……………………… |
| 4 | Parametry pamięci masowej | Dysk SSD PCIe min. 512 GB | Rodzaj dysku …………………….. |
| 5 | Porty zewnętrzne | Na przednim panelu:  - Min. 2 x USB; min. 2 x USB 3.1 Gen. 1 (USB 3.0)  - Min. 1 x Wyjście słuchawkowe/głośnikowe  Na tylnym panelu:  - Min. 2 x USB 2.0; min. 3 x USB 3.1 Gen. 1 (USB 3.0)  - Min. 1 x Wyjście audio  - Min. 1 x RJ-45 (LAN)  - Min. 2 x HDMI  - Min. 1 x Display Port | Rodzaje wejść / wyjść ……………………………. |
| 6 | Porty wewnętrzne (wolne) | - Min. 1 x PCI-e x16  - Min. 1 x PCI-e x1  - Min. 2 x SATA III (wolne) | Rodzaje portów …………….. |
| 7 | Komunikacja przewodowa | Ethernet, obsługująca przepustowości 10/100/1000, ze złączem RJ45 (nie zajmująca portu USB) | TAK/NIE |
| 8 | Karta graficzna | Zintegrowana z płytą główną  Pamięć współdzielona  Możliwość podłączenia jednocześnie min 2 monitorów w rozdzielczościach 1920 x 1200 każdy  Rodzaj wyjść: min 1 HDMI oraz min. 1 Display Port (bez stosowania przejściówek) | TAK/NIE |
| 9 | Napęd optyczny | Wbudowana nagrywarka DVD+/-RW | TAK/NIE |
| 10 | Obudowa | Obudowa fabrycznie konwertowalna typu Small Form Factor z możliwością pracy w pozycji pionowej i poziomej | TAK/NIE |
| 11 | Klawiatura | Załączona do zestawu  Rodzaj komunikacji: przewodowa USB  Układ klawiatury: US  Układ polski znaków: znaki zgodne z układem w MS Windows „polski programisty”  Klawiatura musi być wyposażona w 2 klawisze ALT (prawy i lewy) i blokiem numerycznym | TAK/NIE |
| 12 | Mysz | Załączona do zestawu  Przewodowa optyczna, min. dwa przyciski, jedna rolka, złącze USB, podkładka pod mysz | TAK/NIE |
| 13 | Zainstalowany system operacyjny, oprogramowanie | System operacyjny:  Microsoft Windows 10 Pro wersji dla procesorów 64 bitowych w polskiej wersji językowej lub równoważny pozwalający na:  - podłączenie i użytkowanie nowego sprzętu w istniejącym środowisku opartym o systemy Windows (domena, serwery z drukarkami sieciowymi itp.);  - obsługę programów specjalistycznych, dedykowanych dla jednostek samorządu terytorialnego do pracy w środowisku Windows  - umożliwiający zainstalowanie i korzystanie z ochrony antywirusowej komputera  - umożliwiający uruchomienie przeglądarki internetowej w celu pełnej funkcjonalnie pracy na aplikacjach webowych wdrożonych w jednostkach samorządu terytorialnego zoptymalizowanych pod kątem działania w przeglądarce Internet Explorer  Zamawiający wymaga partycji odzyskiwania pozwalającej na ponowną instalację systemu **niewymagającą** wpisywania klucza rejestracyjnego lub rejestracji poprzez Internet czy telefon.  System operacyjny powinien być oprogramowaniem w wersji najnowszej dostępnej w momencie złożenia ofert.  Zamawiający wymaga, aby w każdym komputerze zainstalowany był system operacyjny samoczynnie aktywujący się kluczem zaszytym w BIOS po podłączeniu do Internetu  Oprogramowanie:  Zamawiający nie dopuszcza wersji oprogramowania ograniczonych czasowo, demo, trial itp. | Nazwa systemu operacyjnego: .............................  Architektura 64 bit: tak / nie |
| 14 | Wymagania dotyczące zasilania | Zasilacz min. 180W | Moc zasilacza …………………………. |
| 15 | Wyposażenie: | Kabel zasilający do PC o długości min. 1m zakończony wtykiem standardowym (wykorzystywanym w Polsce) | TAK/NIE |
| 16 | Wsparcie techniczne | Dostęp do aktualnych sterowników do urządzeń i podzespołów zainstalowanych w komputerze, realizowany poprzez podanie identyfikatora klienta lub modelu komputera lub numeru seryjnego komputera, na dedykowanej przez producenta stronie internetowej. | TAK/NIE |
| 17 | Gwarancja | Warunki gwarancji: Minimum 3-letnia gwarancja producenta komputera liczona od daty dostawy. Serwis urządzeń realizowany przez producenta lub autoryzowanego partnera serwisowego producenta. | Gwarancja …………………………… |

1. ***Dostawa monitorów – 23 sztuki***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, typ, model)*

|  |  |  |
| --- | --- | --- |
| **Poz.** | **Wymagane parametry** | **TAK/NIE\***  **Oferowane parametry\*\*** |
| 1 | Typ ekranu: Ekran płaski, IPS o przekątnej minimum 24” Format ekranu 16:10 | Typ ekranu ……………………………  Format ekranu ……………………………  Przekątna ekranu ………………………. |
| 2 | Rozmiar plamki: maksymalna 0,275 mm | TAK/NIE |
| 3 | Jasność: minimum 250 cd/m2 | Jasność ………………………… |
| 4 | Kontrast: minimum 1000:1 / 5 000 000:1 (dynamic) | Kontrast …………………………… |
| 5 | Kąty widzenia (pion/poziom): minimum 178/178 stopni | Kąty widzenia ……………………….. |
| 6 | Czas reakcji matrycy: maksymalnie 5 ms | Czas reakcji matrycy ………………………… |
| 7 | Aktywny filtr światła niebieskiego | TAK/NIE |
| 8 | Rozdzielczość: minimum 1920 x 1200 (WUXGA) | Rozdzielczość ………………………….. |
| 9 | Powłoka powierzchni ekranu: Matowa | Powłoka ekranu …………………….. |
| 10 | Dodatkowe wyposażenie: Kabel zasilający  Kabel sygnałowy Kabel DisplayPort oraz HDMI o długości minimum 1,5m | TAK/NIE |
| 11 | Złącza: min. 1 x złącze HDMI, min. 1 x złącze DisplayPort, , min. 3 x USB 3.1 Gen. 1 | Rodzaje wejść / wyjść …………………………. |
| 12 | Dźwięk: Dołączony zestaw głośników mocowany do monitora | TAK/NIE |
| 13 | Funkcje dodatkowe:  - Regulacja wysokości ekranu min. 135 mm  - Regulacja pochylenia ekranu w przód i w tył  - Możliwość obracania ekranu (PIVOT)  - Wbudowany zasilacz | TAK/NIE |
| 14 | Standardy i Certyfikaty:  -ENERGY STAR -CE -TCO Certified  lub równoważne. | TAK/NIE |
| 15 | Warunki gwarancji: Minimum 3-letnia gwarancja producenta monitora liczona od daty dostawy. Serwis urządzeń realizowany przez producenta lub autoryzowanego partnera serwisowego producenta. | Gwarancja ………………………………… |

1. ***Dostawa dysków twardych – 8 sztuk***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, typ, model)*

|  |  |  |
| --- | --- | --- |
| **Poz.** | **Wymagane parametry** | **TAK/NIE\***  **Oferowane parametry\*\*** |
| 1 | Pojemność 16 TB | Pojemność ………….. |
| 2 | Format 3,5” | Format ……………… |
| 3 | Złącze SATA III (6.0 Gb/s) | Typ złącza …………………. |
| 4 | Prędkość obrotowa 7200 obr./min | Prędkość obrotowa ………………… |
| 5 | Wielkość bufora min. 512 MB | Bufor …………… |
| 6 | Niezawodność MTBF min. 2 500 000 godzin | Niezawodność ……………. |
| 7 | Dodatkowe informacje: Zgodność z systemami NAS  Kompatybilny z Synology RS815RP+ | TAK/NIE |
| 8 | Standardowa gwarancja producenta min. 5 lat | Gwarancja ……………………. |

1. ***Dostawa dysków zewnętrznych – 2 sztuki***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, typ, model)*

|  |  |  |
| --- | --- | --- |
| **Poz.** | **Wymagane parametry** | **TAK/NIE\***  **Oferowane parametry\*\*** |
| 1 | Pojemność 4 TB | Pojemność ………….. |
| 2 | Format 2,5” | Format ……………… |
| 3 | Złącze USB Micro-B | Typ złącza …………………. |
| 4 | Interfejs USB 3.2 Gen. 1 | TAK/NIE |
| 5 | Kabel USB w zestawie | TAK/NIE |
| 6 | Standardowa gwarancja producenta min. 2 lata | Gwarancja ……………………. |

1. ***Dostawa notebooka – 1 sztuka***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, typ, model)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Poz.** | **Nazwa podzespołu** | **Wymagane parametry** | **TAK/NIE\***  **Oferowane parametry\*\*** |
| 1 | Procesor | Procesor wielordzeniowy, min. 4 rdzenie fizyczne  Minimum—10 000 punktów osiągniętych w teście PassMark CPU Mark  <https://www.cpubenchmark.net/cpu_list.php>  Układ musi pracować z fabrycznymi ustawieniami producenta (niedozwolony tzw. „overlock-ing”) | Producent procesora: …………………………….  Model procesora: …………..….…………………  Częstotliwość procesora: …….………………….  Wynik w testach: …………………………….. |
| 2 | Przekątna ekranu | 15,6'' | TAK/NIE |
| 3 | Typ matrycy | IPS | TAK/NIE |
| 4 | Powierzchnia matrycy | matowa | TAK/NIE |
| 5 | Rozdzielczość | 1920 x 1080 (FHD 1080) | Rozdzielczość …………………………….. |
| 6 | Karta graficzna | Zintegrowana | TAK/NIE |
| 7 | Pamięć RAM | Min. 16GB | Ilość RAM …………….. |
| 8 | Typ i pojemność dysku | Dysk SSD o pojemności min. 512GB | Typ dysku ……………….  Pojemność dysku …………………. |
| 9 | Komunikacja | Min. 1x LAN 10/100/1000, WiFi 802.11 ax, Bluetooth | TAK/NIE |
| 10 | Porty USB | min. 3 x USB 3.0, min. 1 x USB Typu-C (z DisplayPort) | Ilość portów USB ……………………….. |
| 11 | Inne parametry | 1. Kamera internetowa 2. Podświetlana klawiatura 3. Czytnik linii papilarnych | TAK/NIE |
| 13 | Zainstalowany system operacyjny, oprogramowanie | System operacyjny:  Microsoft Windows 10 Pro wersji dla procesorów 64 bitowych w polskiej wersji językowej lub równoważny pozwalający na:  - podłączenie i użytkowanie nowego sprzętu w istniejącym środowisku opartym o systemy Windows (domena, serwery z drukarkami sieciowymi itp.);  - obsługę programów specjalistycznych, dedykowanych dla jednostek samorządu terytorialnego do pracy w środowisku Windows  - umożliwiający zainstalowanie i korzystanie z ochrony antywirusowej komputera  - umożliwiający uruchomienie przeglądarki internetowej w celu pełnej funkcjonalnie pracy na aplikacjach webowych wdrożonych w jednostkach samorządu terytorialnego zoptymalizowanych pod kątem działania w przeglądarce Internet Explorer | Nazwa systemu operacyjnego: .............................  Architektura 64 bit: tak / nie |
| 14 | Pozostałe porty we/wy | 1. Min. 1 x Audio (Combo) 2. Min. 1 x RJ-45 | Pozostałe porty …………………… |
| 17 | Gwarancja | Warunki gwarancji: Minimum 3-letnia gwarancja producenta laptopa liczona od daty dostawy. Serwis urządzeń realizowany przez producenta lub autoryzowanego partnera serwisowego producenta. | Gwarancja …………………………… |

1. ***Dostawa telefonów VoIP – 2 sztuki***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, typ, model)*

|  |  |  |
| --- | --- | --- |
| **Poz.** | **Wymagane parametry** | **TAK/NIE\***  **Oferowane parametry\*\*** |
| 1 | Minimum obsługa 3 kont SIP | Ilość obsługiwanych kont ………….. |
| 2 | Funkcje:  - wstrzymanie/wyciszanie połączeń, DND  - przekierowywanie, połączenia oczekujące, transfer połączeń  - ponowne wybieranie, oddzwanianie, auto odpowiedź  - funkcja głośnomówiąca  - lokalna książka telefoniczna na min. 1000 wpisów  - bezpośrednie połączenie IP bez SIP Proxy  - identyfikacja dzwoniącego (ID) z nazwą i numerem | TAK/NIE |
| 3 | Obsługa dźwięku HD: w słuchawce, w głośniku | TAK/NIE |
| 4 | Obsługa kodeków: min. G.722, G.711(A/μ), G.729AB, G.726, iLBC | TAK/NIE |
| 5 | DTMF: In-band, Out-of-band (RFC 2833) and SIP INFO | TAK/NIE |
| 6 | Graficzny wyświetlacz LCD | TAK/NIE |
| 7 | Wskaźnik LED dla oczekujących połączeń i wiadomości | TAK/NIE |
| 8 | Wybór języka (w tym język polski) | TAK/NIE |
| 9 | Interfejsy:  Min. 2 porty RJ45 Gigabit Ethernet w tym PoE  Min. 1 port RJ9 (4P4C) na słuchawkę ręczną  Min. 1 port RJ9 (4P4C) na zestaw słuchawkowy | TAK/NIE |
| 10 | Zarządzanie:  - konfiguracja : przeglądarka/telefon/auto-provision  - auto-provision przez : FTP/TFTP/HTTP/HTTPS dla masowego wdrożenia  - eksport śledzenia danych, logi systemowe  - blokada telefonu dla ochrony prywatności | TAK/NIE |

1. ***Dostawa modułu rozszerzającego (przystawka sekretarska) do telefonu Yealink T54S lub równoważny***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, typ, model)*

**Wymagane parametry:**

- Duży kolorowy wyświetlacz LCD  
- Min. 20 klawiszy do zaprogramowania aż do 60 różnych funkcji np. BLF/BLA, szybkie wybieranie, odbieranie, przekierowywanie, transfer, parkowanie połączeń  
- Min. 20 fizycznych klawiszy, każdy z dwukolorowym podświetleniem LED  
- niezależne klawisze służące do przewijania stron

1. ***Dostawa licencji (systemu operacyjnego) – 2 sztuki***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, nazwa systemu, wersja)*

Licencja Microsoft Windows Serwer STD CORE 2019 16Lic licencja rządowa CoreLic MOLP lub równoważny spełniający następujące warunki:

1. musi w pełni współpracować ze środowiskiem Active Directory MS Windows Server.

2. licencja musi:

• być nieograniczona w czasie,

• pozwalać na użytkowanie komercyjne,

• pozwalać na instalację nieograniczoną ilość razy,

• możliwość przenoszenia pomiędzy maszynami – licencja nie przypisana do sprzętu.

3. musi mieć możliwość skonfigurowania przez administratora regularnego i automatycznego pobierania i instalowania aktualizacji i poprawek do systemu operacyjnego.

4. darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat),

5. na stronie WWW producenta serwera powinny być dostępne aktualne wersje kompletu sterowników do urządzeń i składników stanowiących wyposażenie dostarczanego urządzenia dla dostarczonego systemu operacyjnego,

6. musi mieć możliwość tworzenia wielu kont użytkowników o różnych poziomach uprawnień, zabezpieczony hasłem dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników,

7. musi być wyposażony w graficzny interfejs użytkownika,

zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika,

8. zintegrowane oprogramowanie dla tworzenia kopii zapasowych (Backup), automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; możliwość przywracania plików systemowych,

9. zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego,

10. musi być w pełni kompatybilny z oferowanym sprzętem,

11. nie może ograniczać możliwości instalacji w przyszłości nowego powszechnie dostępnego sprzętu (sterowniki) oraz oprogramowania, w tym zgodności z oprogramowaniem użytkowanym i zakupionym przez Zamawiającego,

12. oferowany system musi zapewnić nieograniczoną ilość kontenerów środowiska OSE oraz kontenerów Windows Server,

13. oferowany system musi zapewnić ochronę maszyn wirtualnych, usługę ochrony hosta, replikę magazynu oraz umożliwiać tworzenie magazynów danych zdefiniowanych programowo.

1. **Dostawa akumulatora do UPS zgodnego z UPS APC 650 (BK650EI) lub równoważny – 10 sztuk**
2. **Dostawa zestawu akumulatorów do UPS zgodnego z APC Smart-UPS 1500 VA, LCD, 230 V (SMT1500I) lub równoważne – 1 sztuka**
3. **Dostawa modułu SFP+ 10gb zgodnego z serwerem HP DL360 G10 lub równoważny – 4 sztuki**
4. **Dostawa modułu SFP+ 10gb zgodnego z serwerem HP DL380 G9 lub równoważny – 2 sztuki**
5. **Dostawa karty sieciowej SFP+ 10gb (min. 2 porty SFP+) zgodnej z serwerem HP DL380 G9 lub równoważnej – 1 sztuka**

**Zadanie nr 3 Dostawa urządzenia wielofunkcyjnego formatu A3**

1. ***Dostawa kolorowego urządzenia wielofunkcyjnego – 1 sztuka***

………………………………………………………………………………………………………

………………………………………………………………………………………………………

*(nazwa producenta, typ, model)*

Wymagane parametry techniczne urządzeń w modułach

|  |  |
| --- | --- |
| Parametr | Wymagania dla modułu A3 |
| Rodzaj urządzenia | Kolorowe urządzenie wielofunkcyjne (kopiarka, skaner i drukarka), mobilne (na kółkach), zintegrowane w jednej obudowie, nie wymagające dodatkowego komputera obsługującego proces kopiowania |
| Technologia wydruku | Laserowa, tonerowa (kolorowa) |
| Podajnik dokumentów | Podajnik oryginałów na min. 270 arkuszy przy gramaturze 80 g/m2 . Podajnik obsługujący papier o gramaturze od 50 do 220 g/m2 |
| Interfejsy | USB 3.0 (Super-Speed USB), 4 x USB Host  Interface, Gigabit Ethernet(10BaseT/100BaseTX/1000Bas  eT, IPv6, IPv4, IPSec, 802.3az) |
| Maksymalna wielkość wydruku lub dokumentu skanowanego | A3 (420 x 297 mm) |
| Minimalna prędkość druku | Mono/kolor : 40 arkuszy A4 na minutę |
| Obsługiwana gramatura | Od 52 do 300g/m2 |
| Podajniki | 2 kasety x 500 ark. A4 i A3, oraz podajnik boczny |
| Odbiornik wydruków | Taca ręczna |
| Rodzaj skanera | Dwustronne jednoprzebiegowe skanowanie |
| Rozdzielczość optyczna skanowania i wydruków | Skanowanie – min. 600 dpi  Wydruk – min. 1200 dpi |
| Format skanowanych dokumentów | TIFF, JPEG, Open XPS, PDF oraz PDF „przeszukiwany” (OCR) |
| Dysk twardy | Min. 320gb z możliwością szyfrowania oraz bezpiecznego nadpisywania danych |
| Pamięć RAM | Min. 4 GB |
| Możliwe źródła wydruku – wybór z panelu urządzenia | Zasoby sieci komputerowej, dysk twardy urządzenia, pamięć USB, |
| Miejsca (cel) skanowania – wybór z panelu urządzenia | Zasoby sieci komputerowej, dysk twardy urządzenia, pamięć USB, e-mail, Network TWAIN |
| Pobór mocy w trybie drukowania | 780W |
| Maksymalny pobór mocy w trybie uśpienia | 0,8W |
| Wymiary i waga urządzenia | Maks. szerokość 602mm  Maks. głębokość 665mm  Maks. wysokość 790mm  Maks. waga 96 kg |
| Zarządzanie | - panel operatorski wielodotykowy, z możliwością dowolnej konfiguracji ikon typu: Drukarka / Kopiarka / Skaner / Serwer dokumentów  - przeglądarka internetowa |
| Personalizacja | Personalizacja panelu głównego oraz możliwość dopasowania do wymagań użytkowników, kody PIN dla użytkowników, znak wodny, stempel, numery stron. |
| Czas nagrzewania po uśpieniu | Maks. 17 sekund |
| Wyposażenie dodatkowe | Pakiet produkcyjnych materiałów eksploatacyjnych (tonerów o maksymalnej dostępnej pojemności) oprócz zestawu startowego oraz oryginalny stolik na kółkach pod urządzenie |
| Szablony użytkownika | Użytkownik może tworzyć i użytkować własne szablony drukowania lub skanowania |
| Obciążenie miesięczne | Min. 150 000 wydruków A4 |
| Gwarancja | 24 miesięce |

**\*** - niepotrzebne skreślić

\*\* - wpisać parametry oferowanego sprzętu, z których musi wynikać spełnienie wymagań.