Spis treści

1. Wprowadzenie

Przedmiotem zamówienia jest dostawa i wdrożenie nowych rozwiązań z zakresu bezpieczeństwa sieci, tj.: zapora ogniowa, ochrona antywirusowa, połączenia typu VPN z zabezpieczeniami SSL i IPSec, zabezpieczenia typu IDS/IPS. Elementem zamówienia jest także reorganizacja, rozbudowa infrastruktury sieciowej oraz serwerowej pod kątem bezpieczeństwa sieciowego i utraty danych.

2. Cel

Podstawowym celem projektu jest Zwiększenie bezpieczeństwa i niezawodności środowiska informatycznego Wojewódzkiego Inspektoratu Transportu Drogowego w Bydgoszczy.
Nowo dostarczane rozwiązanie sprzętowe posłuży, jako podstawa do reorganizacji całego środowiska organizacji WITD. W rama zamówienia należy dostarczyć, zaprojektować a następnie wdrożyć oferowane rozwiązanie wraz z usługami towarzyszącymi.

3. Wymagania sprzętowe do realizacji przedmiotu zamówienia

Do wykonania przedmioty zamówienia wymagany jest sprzęt:

Wymagania w zakresie nowego rozwiązanie sprzętowego klasy UTM:

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. Powinna istnieć możliwość dedykowania 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

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

Interfejsy, Dyski:

- Nie mniej niż 2 porty WAN Ethernet Interfaces 10/100/1000 Base-TX, 2 dodatkowe porty SFP z możliwością współdzielenia z portami WAN.
- System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
- Nie mniej niż 2 porty pozwalające na zarządzanie dedykowanymi przełącznikami.

Parametry wydajnościowe:

- W zakresie Firewall'a obsługa nie mniej niż 1,5 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.
- Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
- Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,8 Gbps.
- Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA1: nie mniej niż 6,5 Gbps.
- Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 1,9 Gbps.
- Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
- Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http przy zastosowaniu różnych szyfrowań – minimum 715 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

- Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
- Kontrola Aplikacji.
- Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
- Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
- Ochrona przed atakami - Intrusion Prevention System.
- Kontrola stron WWW.
- Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.

- Zarządzanie pasmem (QoS, Traffic shaping).
- Analiza ruchu szyfrowanego protokołem SSL oraz SSH.
- Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
- 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.

Polityki, Firewall

- System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW.
- Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
- 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.
- W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

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 Diffiego-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

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.
- Dla modułów: IPSec VPN oraz SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. Klient VPN musi umożliwiać weryfikację stanu bezpieczeństwa stacji zdalnej.
- sRozwiązanie powinno zapewniać funkcjonalność VTEP (VXLAN Tunnel End Point)

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.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

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

Kontrola Antywirusowa

- Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
- System musi umożliwiać skanowanie archiwów, w tym, co najmniej: zip, RAR.

- Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

Ochrona przed atakami

- Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
- Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
- System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
- 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.

Kontrola aplikacji

- Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- Baza Kontroli Aplikacji powinna zawierać minimum 2800 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
- Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P, Botnet.
- Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

- Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
- W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware, phishing, spam, Dynamic DNS, proxy avoidance.
- Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

- Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
- 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.
- Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

- 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.
- Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
- Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

- 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.
- Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
- Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
- System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
- System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

- System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie:

- System musi mieć możliwość logowania 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.
- W ramach logowania system 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.
- Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
- Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:

- ICSA lub EAL4 dla funkcji Firewall
- ICSA lub NSS Labs dla funkcji IPS
- ICSA dla funkcji: SSL VPN, IPSec VPN

Serwisy i licencje

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

- Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 36 miesięcy.

Gwarancja oraz wsparcie

- 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 8x5.

Gwarancja/AHB:

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.

Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty:

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

Wymagania w zakresie nowego rozwiązanie serwerowego

Obudowa	· Typu Rack, wysokość maksimum 1U; · Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack oraz ramieniem porządkującym ułożenie przewodów w szafie rack; · Obudowa umożliwiająca instalację do 10 dysków
Płyta główna	· jednoprocesorowa, możliwość instalacji procesorów minimum sześćdziesięcioczterordzeniowych; · Wyposażona w minimum 16 gniazd pamięci RAM DDR4, obsługa minimum 1TB pamięci RAM DDR4 min. 3200 Mhz; · Możliwość zainstalowania minimum dwóch dysków M.2 SATA o pojemności min. 240GB oraz możliwość konfiguracji w RAID 1.
Procesor	· Zainstalowany minimum jeden procesor 16 rdzeniowy, min. 64 MB cache o taktowaniu podstawowym min. 2.8GHz o wydajności osiągającej w teście PassMark PerformanceTest co najmniej wynik 31500 punktów PassMark CPU Mark (wynik zaproponowanego procesora musi aktualnie znajdować sie na stronie http://www.cpubenchmark.net)
Pamięć RAM	· Zainstalowane minimum 128 GB pamięci RAM typu DDR4 Registered, min. 3200MHz w kościach o pojemności min. 64GB
Kontrolery dyskowe, I/O	· Kontroler SAS/SATA, obsługa minimum 8 dysków hot-plug RAID 0,1,5,6,10,50,60 · Wyposażony w 8GB NV Cache · Zainstalowane minimum pięć dysków 3.5” lub 2.5” SSD SATA 6Gb min. 960GB każdy
Sloty	Serwer musi być wyposażony w min. 2 sloty PCI-Express x16 low-profile
Bezpieczeństwo	Serwer musi zostać wyposażony w zintegrowany z płytą główną moduł TPM 2.0
Kontrolery LAN	· Minimum jedna czteroportowa karta 1Gbit/s ze wsparciem iSCSI, niezajmująca slotu PCI Express, zintegrowana z płytą główną serwera · Minimum jedna dodatkowa karta dwuportowe 10GbE SFP+ ze sprzętowym wsparciem dla wirtualizacji
Porty wbudowane	· Zintegrowana karta graficzna · Min. 1x USB 2.0 dostępne na froncie obudowy · Min. 2x USB 3.0 dostępne z tyłu serwera

	· Min. 1x USB 3.0 wewnątrz serwera · Min. 2x VGA z czego jeden na froncie obudowy · Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera · Min. 1x RS-232 (DB9)
Zasilanie, chłodzenie	· Redundantne dwa zasilacze hotplug o mocy minimum 550W Platinum · Redundantne wentylatory hotplug;
Zarządzanie	Serwer wyposażony w kartę zarządzającą, działającą niezależnie od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: · Monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe · Wparcie dla agentów zarządzających oraz możliwość pracy w trybie bez agentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP · Dostęp do karty zarządzającej poprzez: o Dedykowany port RJ45 z tyłu serwera · Dostęp do karty możliwy o Z poziomu przeglądarki webowej (GUI) o Z poziomu linii komend o Poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) · Wbudowane narzędzia diagnostyczne · Zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego · Obsługa mechanizmu automatycznego połączenia karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie · Wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników · Przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)

	· Obsługa zdalnego serwera logowania (remote syslog) · Wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów, uruchamiana w przeglądarce www bez potrzeby instalowania rozszerzeń (minimalne wersje Firefox 76, Chrome 81) · Monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji · Konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) · Zdalna aktualizacja oprogramowania (firmware) · Możliwość równoczesnej obsługi przez 6 administratorów · Autentykacja dwuskładnikowa (Kerberos) · Wsparcie dla Microsoft Active Directory · Obsługa TLS i SSH · Wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API · Wsparcie dla zdalnego graficznego dostępu pod systemem Windows Server z obsługą klawiatury, myszy i wirtualnych mediów Zamawiający dopuszcza rozwiązanie równoważne do Integrated Remote Console for Windows clients · Możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wspierane OS	Min.: Windows 2016, Windows 2019, VMWare, Suse, RHEL. Potwierdzeniem spełnienia wymogu będzie wpis na stronie producenta danego systemu operacyjnego, tzw. HCL.
Gwarancja	Minimum 36-cio miesięczny okres gwarancji i wsparcia technicznego świadczonego w miejscu instalacji. Okno czasowe zgłaszania incydentów dotyczących sprzętu - 24/7 Czas naprawy sprzętu: najpóźniej w następnym dniu roboczym od momentu wykrycia awarii.

Inne wymagania	Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji i dostarczona
Licencje dostępowe	Dodatkowo należy dostarczyć 50 licencji dostępowych dla użytkowników zgodnych z Windows 2019
System operacyjny	Dostarczona licencja pozwalająca na zainstalowanie oraz poprawną pracę systemu operacyjnego Windows Server 2019 w wersji Standard. Licencja obejmująca wszytkie rdzenie zainstalowanego procesora Dostarczona dodatkowa licencja systemu operacyjnego Windows Server 2019 w wersji Standard pozwalająca na uruchomienie dodatkowych dwóch instancji wirtualnych opartych o systemy Windows Server Dostarczony nośnik z systemem operacyjnym

Wymagania w zakresie nowego rozwiązania pamięci masowej opartej o taśmy magnetyczne

Typ urządzenia	Biblioteka taśmowa LTO8
Obudowa	Rack 19 ‘’ Wysokość – max 1U Zainstalowany mechanizm do automatycznej zmiany taśm Możliwość obsługi minimum jednego napędu taśmowego LTO-8 Przystosowana do jednoczesnego załadowania minimum 9 taśm LTO-8 zainstalowany czytnik kodów kreskowych służący do identyfikacji taśm wbudowany wyświetlacz LCD sygnalizujący stan pracy urządzenia
Ilość zainstalowanych napędów	Minimum 1 zainstalowany napęd LTO-8 SAS
Typ zainstalowanego napędu taśmowego	Pojemność natywna obsługiwanych taśm 12 TB obsługa kompresji danych minimum 2,5:1
Zdalne zarządzanie	Minimum 1 x złącze FastEthernet lub minimum 1 x Gigabit Ethernet przeznaczone do zdalnego zarządzania.
Ilość dostarczonych taśm LTO	Min. 15 sztuk taśm LTO-8 RW Min. 1 taśma czyszcząca (Universal Cleaning Cartridge)
Dodatkowe wymagania	Należy dostarczyć osprzęt (szyny montażowe) do zamontowania biblioteki taśmowej w szafir RACK 19 ‘’ Komplet kabli zasilających Należy dostarczyć kontroler EX-SAS, który będzie elementem rozbudowy serwera Fujitsu RX300 S8 posiadanego przez Zamawiającego Należy dostarczyć przewód do połączenia biblioteki taśmowej z serwerem o długości 4m

Obsługiwane systemy operacyjne, licencje i sterowniki	Należy dostarczyć wymagane sterowniki do wykorzystania pełnej funkcjonalności biblioteki taśmowej do systemu Windows server standard 2019 Biblioteka musi występować na liście zgodności „Backup Exec 21 - 21.x Hardware and Cloud Storage Compatibility List (HCL)”
Gwarancja	Minimum 36-cio miesięczny okres gwarancji i wsparcia technicznego świadczonego w miejscu instalacji. Okno czasowe zgłaszania incydentów dotyczących sprzętu - 24/7 Czas naprawy sprzętu: najpóźniej w następnym dniu roboczym od momentu wykrycia awarii.

Wymagania w zakresie nowego rozwiązanie oprogramowania backup-u

Rozbudowa oprogramowania BackupExec 21 Vray wraz z niezbędnymi licencjami zapewniającymi obsługę:

- Jeden host fizyczny pełniący rolę serwera wirtualizacji – Hyper-V
- Pięć hostów wirtualnych pełniących rolę serwerów aplikacji typu SQL, itp.

Wymagania minimalne:

Oprogramowania do Backupu	O parametrach nie gorszych niż:
Licencja	Licencja pełna, nieograniczona czasowo pozwalająca na instalację oprogramowania na dedykowanym serwerze backupu oraz tworzenie kopi z dwóch hostów fizycznych pełniący rolę serwer wirtualizacji – Hyper-V; czterech hostów wirtualnych pełniących rolę serwerów aplikacji typu SQL; jednego hosta fizycznego z systemem Linux pełniącego rolę serwera poczty; jednego hosta fizycznego z systemem Windows Server pełniącego rolę serwera poczty,
Funkcjonalność	Oprogramowanie umożliwiające wykonywania kopii zapasowych serwerów wirtualnych pracujących w środowisku wirtualizacyjnym Hyper-V
	Obsługa systemów operacyjnych Windows Server 2012, Windows Server 2012 R2, Windows Server 2016. Windows Server 2019
	Przywracanie maszyn wirtualnych, aplikacji, baz danych, plików, folderów z pojedynczej kopii zapasowej
	Backup maszyn wirtualnych bez użycia agentów zainstalowanych w systemach gościa
	Konsola administracyjna
	Ochrona systemów operacyjnych, platform, aplikacji i baz danych w środowiskach wirtualnych i fizycznych z obsługą dysków i pamięci taśmowych (RDX, LTO) a także z obsługą hostów zewnętrznych takich jak: AWS (Amazon Web Service), Gateway VTL

	Zintegrowane przywracanie typu Bare-Metal
	Zastosowanie mechanizmów deduplikacji
	Ochrona nieograniczonej liczby maszyn wirtualnych per węzeł
	Odzyskiwanie całego systemy na tym samym sprzęcie lub innym
	Konwersja kopii zapasowych do maszyn wirtualnych (B2V, P2V)
	Konwersja kopii zapasowych do maszyn fizycznych (V2P)
	Restore Wizard
	Validator maszyn wirtualnych
	Wbudowany mechanizm DR dla systemów wirtualnych oraz fizycznych.
	Powiadomienia – poprzez wiadomości e-mail lub SMS w momencie wystąpienia alarmu. Obsługa SMTP authentication
	Zintegrowane usuwanie skutków awarii
	Zintegrowane funkcje przywracania systemu w trybie „Bare-Metal Restore” oraz „bez sprzętowego” usuwania awarii

4. Zakres prac

W zakresie obecnego środowiska Zamawiającego:

- Wykonawca przeprowadzi pod nadzorem Zmawiającego audyt obecnego środowiska na podstawie, którego przygotuje projekt wdrożenia, zakres urządzeń podlegających audytowi:
    - Klaster niezawodnościowo/wydajnościowych założony z dwóch przełączników zarządzalnych Cisco WS-3750X z uruchomionymi usługami/funkcjami: VLAN, VTP, RSTP, LAG, Trunking,
    - UTM FortiGate 80F
    - Serwery fizyczne i wirtualne

W zakresie instalacji i uruchomienia dostarczanego rozwiązania klasy UTM:

- Wykonawca dostarczy oraz zamontuje elementy wraz ze wyspecyfikowanymi akcesoriami w pomieszczeniach wskazanych przez Zamawiającego.
- Konfiguracja dostarczonego urządzenia/urządzeń zapewniająca poprawną współpracę w obecnej konfiguracji sieci, Zmawiający oczekuje:
    - Odwzorowania ustawień adresacji dla interfejsów (LAN, WAN, VLAN, DMZ, itp.)
    - Odwzorowania ustawień aktualnych polityk bezpieczeństwa na firewall-u wraz z ustawieniami filtrów aplikacji, treści, itp.
    - Odwzorowanie ustawień mapowania i przekierowania portów
    - Odwzorowanie ustawień kontrolera sieci bezprzewodowej
    - Odwzorowanie konfiguracji serwera VPN korzystającego z bazy użytkowników znajdujących się w Active Directory
- Wykreowanie VLAN-ów wraz z podziałem na podsieci i readresacją środowiska sieciowego Zamawiającego. Zamawiający oczekuje utworzenie minimum 8 VLAN-ów, do których należy przydzielić adresy IP różnych podsieci, według zasady:
    - Przykład 1 - VLAN 110 – adres IP 192.168.110.1
    - Przykład 2 - VLAN 111 – adres IP 192.168.111.1

  Dokładne numery VLAN-ów oraz przynależące adresy zostaną skonfigurowane po akceptacji projektu wykonawczego (opisane w pkt 6)
- Konfiguracja serwera DHCP dla każdego wykreowanego VLAN-u/podsieci
- Konfiguracja polityk bezpieczeństwa w zakresie komunikacji między VLAN-ami - skonfigurowane po akceptacji projektu wykonawczego (opisane w pkt 6)
- Wygenerowanie backup-ów ostatecznej wersji ustawień
- Wygenerowanie backup-ów ostatecznej wersji ustawień

W zakresie instalacji i uruchomienia dostarczanego serwera wraz z oprogramowaniem.

W zakresie serwera :

- Wykonawca przygotuję serwer zgodnie z wymaganiami:
    - Aktualizacja oprogramowania układowego oraz komponentów serwera do najnowszej wersji dostępnej na dzień instalacji
    - Konfiguracja kontrolerów dysków do działaniu w trybie RAID – konfiguracja po akceptacji przez Zamawiającego

- Konfiguracja BIOS-u pod kątem uzyskania odpowiedniej wydajności oraz zwiększeniu bezpieczeństwa
- Konfiguracja modułu zarządzania wraz z usługą mailowego powiadamiania o zdarzeniach
- Instalacja systemu operacyjnego z rodziny Microsoft Windows Server wraz ze wszystkimi aktualizacjami dostępnymi na dzień instalacji
- Instalacja oraz konfiguracja oprogramowania dedykowanego przez producenta serwerów
- Instalacja oprogramowania antywirusowego (licencja dostarczona przez zamawiającego)
- Instalacja i konfiguracja działa w ramach Domeny Active Directory

W zakresie obecnego środowiska serwerowego

- Migracja obecnego serwera fizycznego pełniącego rolę głównego kontrolera domeny Active Directory, serwera DHCP, serwera DNS, serwera plików do maszyn wirtualnych z rozdzieleniem ról.
  Jeden serwer wirtualny główny kontroler domeny Active Directory, serwer DHCP, serwer DNS.
  Drugi serwer wirtualny jako serwer plików.
- Podniesienie funkcjonalności domeny i lasu Active Directory do najnowszej Windows Server 2019.
- Migracja maszyn wirtualnych z obecnego serwera na nowy serwer.
- Przygotowanie obecnego serwera fizycznego Zamawiającego do roli serwera kopii zapasowych
  - Instalacja systemu operacyjnego na serwerze,
  - Aktualizacja podzespołów serwera
  - Aktualizacja systemu operacyjnego
  - Instalacja i konfiguracja oprogramowania kopii zapasowych wraz z implementacją biblioteki taśmowej LTO
  - Kopia zapasowa powinna obejmować całe środowisko serwerowe Zamawiającego.
  - Konfiguracja zadań kopii zapasowych obejmujących kopie na lokalną przestrzeń dyskową i duplikację na taśmy LTO
  - Harmonogram zadań kopii do ustalenia z Zamawiającym

- Zmiana konfiguracji połączenia VPN. Obecnie serwer VPN skonfigurowany na serwerze MS Windows. Należy przenieść konfigurację użytkowników do konfiguracji VPN na urządzeniu UTM

5. Wykonanie przedmiotu zamówienia.

W zakresie uruchomienia urządzenia UTM

a) **Projekt wykonawczy**
   - Na podstawie wymagań Zamawiającego, wykonawca stworzy projekt wykonawczy na podstawie, którego po akceptacji Zamawiającego będą wykonywane wszystkie czynności wdrożeniowe. Projekt wykonawczy powinien zawierać:
     - Opis proponowanego rozwiązania
     - Sposób realizacji – plan wdrożenia opisujący proponowane metody, mechanizmy dla poszczególnych elementów sieci LAN.
     - Schemat graficzny przedstawiający środowisko docelowe.

b) **Harmonogram**
   - Wykonawca w porozumieniu z Zamawiającym utworzy harmonogram realizacji, który będzie podlegał ostatecznej akceptacji przez Zamawiającego

c) **Dokumentacja**
   - Wykonawca stworzy dokumentacja powykonawczą przedstawiającą wdrożone rozwiązanie z uwzględnieniem schematów działania podczas awarii wymaganych przez zamawiającego w zakresie urządzenia UTM.

d) **Testy i weryfikacja**
   - Zamawiający przy asyście wykonawcy na podstawie opisanych wymogów, projektu wykonawczego oraz dostarczonej dokumentacji dokona sprawdzenia poprawności wykonania wdrożenia. Testowane elementy to między innymi:
     - Poprawność działania VLAN- ów
     - Poprawność działania połączeń VPN
     - Poprawność działania autoryzacji hostów
     - Poprawności działania polityk bezpieczeństwa zapory ogniowej

W zakresie konfiguracji serwera, pamięci masowej wraz z oprogramowaniem

a) **Projekt wykonawczy**
   - Na podstawie wymagań Zamawiającego, wykonawca stworzy projekt wykonawczy na podstawie, którego po akceptacji Zamawiającego będą wykonywane wszystkie czynności wdrożeniowe. Projekt wykonawczy powinien zawierać:
     - Opis proponowanej konfiguracji nowo dostarczanego serwera
     - Opis możliwych do wykonania sposobów realizacji backupu (offline, online, przyrostowo, różnicowo, itp.) dla poszczególnych elementów
     - Sposób realizacji – plan wdrożenia opisujący proponowane metody, mechanizmy backupu dla poszczególnych elementów.
     - Kalkulacje wymaganej przestrzeni do wykonania backupu dla poszczególnych elementów.
     - Proponowany harmonogram wykonywania backupu dla poszczególnych elementów wraz z kalkulacją wymaganego czasu.
     - Schemat graficzny przedstawiający środowisko docelowe.

b) **Harmonogram**
   - Wykonawca w porozumieniu z Zamawiającym utworzy harmonogram realizacji, który będzie podlegał ostatecznej akceptacji przez Zamawiającego

e) **Instalacja i konfiguracja systemu Backup-u**
   - Instalacja na istniejącej, produkcyjnego maszynie, dostarczonego oprogramowania do tworzenia backupu. Uwzględniając instalację najnowszej dostępnej wersji oprogramowania na dzień wykonywania prac.
   - Instalacja i konfiguracja odpowiednich elementów zapewniających poprawną współprace z środowiskiem Active Directory zamawiającego.
   - Konfiguracja do pracy z dostarczaną pamięcią masową
   - Instalacja i konfiguracja odpowiednich elementów zapewniających poprawną współpracę z środowiskiem Zamawiającego, a dostarczonym oprogramowaniem przez wykonawcę. Przez poprawną współpracę zamawiający ma na myśli integrację systemu backupu do poziomu w którym będzie możliwość wykonywania backupu całego serwera, poszczególnych jego ról, a także pojedynczych usługi każdej roli, np. SQL Server.
   - Wykonawca na podstawie uzgodnień oraz akceptacji zamawiającego utworzy harmonogram wykonywania backup w skład którego wchodzą:
     - Środowiska serwerowego wraz z rolami i usługami
     - Serwery pełniące inne funkcje

c) **Dokumentacja**
   - Wykonawca stworzy dokumentacja powykonawczą przedstawiającą wdrożone rozwiązanie.

d) Testy i weryfikacja

- Zamawiający przy asyście wykonawcy na podstawie opisanych wymogów, projektu wykonawczego oraz dostarczonej dokumentacji dokona sprawdzenia poprawności wykonania wdrożenia.

6. Wymagania dotyczące wiedzy i doświadczenia wykonawcy.

Zamawiający wymaga od wykonawcy wiedzy i doświadczenia z zakresu obsługi urządzeń:

- **UTM z rodziny Fortinet**
  Potwierdzeniem spełnienia tego wymogu będzie inżynier z certyfikatem NSE4 lub wyższym/nowszym
- **Przełączników z rodziny Cisco w tym także działających w konfiguracjach wysokiej dostępności H/A**
  Potwierdzeniem spełnienia tego wymogu będzie inżynier z certyfikatem CCNA lub wyższym/nowszym
- **Serwerów oparty o oprogramowanie Microsoft Windows Server** działających w konfiguracjach wysokiej dostępności H/A
  Potwierdzeniem spełnienia tego wymogu będzie inżynier z certyfikatem 70-659 lub wyższym/nowszym

7. Gwarancje.

Dostarczony przez wykonawcę sprzęt powinien zostać objęty gwarancją producenta na okres min. 3 lat z możliwością wydłużenia poprzez zakup odpowiednich polis.

Wykonawca udzieli gwarancji na wdrożone rozwiązanie, którego okres minimalny to 12 miesięcy z możliwością przedłużenia.

Obszar gwarancji dotyczy poprawnego działania środowiska, przy uwzględnieniu:
- mechanizmów wydajnościowo/niezawodnościowych wdrożonego środowiska sieciowego
- poprawności wykonywania konfiguracji rozwiązania backupu i replikacji

Wykonawca nie odpowiada za poprawność działania aplikacji uruchomionych w środowisku, o ile nieprawidłowości w działaniu aplikacji nie są spowodowane problemami wynikającymi nieprawidłowościami w działaniu dostarczonego rozwiązania.

Wykonawca udziela również wsparcia technicznego dla dostarczonego rozwiązania w ilości 40 h do wykorzystania w okresie 14 dni roboczych po implementacji rozwiązania, oraz 60 h przez okres trwania gwarancji na wdrożone rozwiązanie.

Po zaimplementowaniu rozwiązania zostanie one przetestowane przy obecności zamawiającego.

Naprawy gwarancyjne:

- Czas reakcji na zgłoszone awarie 4 godziny w dni pracujące w godzinach 7.30-15.30
- W przypadku awarii krytycznych czas reakcji 4 h od zgłoszenia także poza godzinami 7.30-15.30 oraz 4 h w dni wolne od pracy,
- Interwencje zgłoszone, jako gwarancyjne a niewchodzące w obszar gwarancji zostaną zaliczone na poczet wsparcia technicznego

Przez czas reakcji zamawiający uważa podjęcie realnego działania w celu naprawy zaistniałego problemu.