1) Na realizację zadania składają się następujące elementy :
   a) Dostawa urządzenia UTM
   b) Instalacja i konfiguracja urządzenia UTM
   c) Dostawa instalacja i konfiguracja systemu do wirtualizacji, utworzenie dwóch maszyn wirtualnych
   d) Migracja posiadanych serwerów na maszyny wirtualne
   e) Przeprowadzenie szkoleń dla personelu Zamawiającego w zakresie administrowania i użytkowania wdrażanych rozwiązań, oraz wsparcie serwisowe
2) Szczegółowy opis wymagań wyżej wymienionych elementów został przedstawiony w dalszej części niniejszego dokumentu.
3) Jeżeli opis przedmiotu zamówienia wskazywałby w odniesieniu do niektórych produktów lub usług dostarczanych przez konkretnego Wykonawcę znaki towarowe, patenty lub pochodzenie, źródło lub szczególny proces - Zamawiający, zgodnie z art. 29 ust. 3 ustawy Pzp., dopuszcza oferowanie rozwiązań równoważnych. Produkty lub usługi pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, jakim muszą odpowiadać produkty lub usługi oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Produkty lub usługi pochodzące od konkretnych producentów stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Pod pojęciem „minimalne parametry jakościowe i cechy użytkowe" zamawiający rozumie wymagania dotyczące produktów lub usług zawartych w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów/produktów ma wyłącznie charakter przykładowy, a wskazaniu takiemu towarzyszą wyrazy „lub równoważny". Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt lub usługę przy opisie przedmiotu zamówienia, dopuszcza jednocześnie rozwiązania równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu lub usługi, uznając tym samym każdy produkt lub usługę o wskazanych lub lepszych parametrach.

Dostawa urządzenia UTM – minimalne wymagania:

Funkcje modułu Firewall:

1. Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
2. Możliwość uruchomienia w formie klastra wysokiej dostępności (HA) - co najmniej Active-Passive.
3. Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
4. Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.
5. Musi obsługiwać Multicast routing.
6. Musi obsługiwać Policy Based routing.

7. Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.
8. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
9. Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.
10. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
11. Musi obsługiwać Dynamic DNS.
12. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
13. Musi obsługiwać translację portów: PAT.
14. Musi obsługiwać IPSec NAT traversal.
15. Musi obsługiwać mechanizm Policy Based NAT.
16. Musi obsługiwać VLAN 802.1Q.
17. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
18. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
19. Musi mieć możliwość obsługi zapasowego łącza typu LTE poprzez podłączenie zewnętrznego modemu USB.
20. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
21. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.
22. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza.
23. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
24. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
25. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.
26. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.
27. Co najmniej dwie metody transparentnej autoryzacji nie wymagają instalacji dedykowanego agenta na stacjach roboczych użytkowników.
28. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.
29. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
30. Musi dostarczać mechanizmów identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
31. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
32. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
33. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych – dla najpopularniejszych protokołów.
34. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
35. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.

36. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.
37. Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
38. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.
39. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.

Specyfikacja UTM:

1. Firewall musi zapewnić obsługę na poziomie minimalnym:5.8 Gbps dla pracy w trybie firewall,1.18 Gbps dla pracy w trybie full scan (włączone mechanizmy bezpieczeństwa takie jak: AV, IPS)
2. Ilość obsługiwanych sieci VLAN: 100
3. Firewall musi obsługiwać 3 500 000 jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną 34 000 połączeń na sekundę.
4. Minimalna ilość portów 8x 10/100/1000 BaseT oraz 2x SFP+
5. Wsparcie połączeń VPN site-to-site lub client-to-site dla minimum 75 użytkowników.
6. Minimalna ilość uwierzytelnionych użytkowników: 500.

Dostarczony system bezpieczeństwa (UTM) musi zapewniać:

1. Ochronę z wykorzystaniem mechanizmów IPS.
2. Ochronę antywirusową.
3. Ochronę przed niechcianą pocztą.
4. Kontrolę wykorzystywanych aplikacji.
5. Możliwość filtrowania URL.

W ramach ochrony przed atakami system musi zapewniać:

1. Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 8000 definicji sygnatur.
2. Automatyczne blokowanie znanych źródeł ataków.
3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).
5. Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer OverFlow, Remote File Inclusions.
6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.

W ramach kontroli antywirusowej system musi zapewniać:

1. Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie

2. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.
3. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.
4. Możliwość skanowania plików o rozmiarze co najmniej 20MB.
5. Możliwość zdefiniowania rozmiaru skanowanego pliku.
6. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
7. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
8. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.
9. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.

W ramach kontroli antyspamowej system musi zapewniać:

1. Analizę wiadomości pocztowych w oparciu o technologię Recurrent Pattern Detection.
2. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.
3. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
4. Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
5. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.

W ramach filtrowania zawartości URL system musi zapewniać:

1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
2. Baza filtra url powinna zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
3. Odpytywanie bazy on-line w czasie rzeczywistym.
4. Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym, dlaczego dostęp do strony www został zablokowany.
5. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
6. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
7. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.
8. Możliwość określenia różnego rodzaju akcji dla połączeń do wybranych adresów URL na podstawie reputacji.
9. Możliwość filtrowania treści w oparciu o typy MIME.
10. Możliwość blokowania plików cookies dla określonych domen.
11. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
12. Analizę treści dla protokołu https.
13. Wyłączenie inspekcji https dla wybranych kategorii stron www.

W ramach kontroli aplikacyjnej system musi zapewniać:

1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
2. Ilość rozpoznawanych aplikacji: nie mniej niż 1000, podzielonych na kategorie.

3. W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
4. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.

Wymagane funkcje VPN systemu:

1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
5. Obsługa Dead Peer Detection (DPD).
6. Wsparcie dla IKEv1 i IKEv2.
7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.
10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.
12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.

Zarządzanie:

1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.

7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.
8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.

Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania:

1. Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
2. Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
3. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
4. Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
5. Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
6. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
7. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
8. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
9. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
10. Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
11. Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
12. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
13. Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
14. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
15. System ma mieć możliwość generowania raportów w formacie PDF oraz opcję eksportowania szczegółowych informacji do pliku CSV.
16. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
17. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
18. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
19. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
20. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
21. Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.

Ochrona stacji końcowych:

1. Licencja musi obejmować ochronę stacji końcowych w formie agentów (minimum 75).
2. Rozwiązanie musi pochodzić od producenta rozwiązania.
3. Rozwiązanie musi minimum: ochraniać przed oprogramowaniem ransomware, posiadać zaawansowane techniki ochrony przed złośliwym oprogramowaniem, posiadać ochronę antytamperową, aktualizować sygnatury i heurystykę.

a) Instalacja i konfiguracja urządzenia UTM

W ramach zadania Wykonawca:

- zainstaluje dostarczone urządzenie UTM,
- przeniesie wszystkie polisy i konfiguracje z obecnego urządzenia PALO ALTO,
- podepnie wszystkie posiadane i wymagane łącza internetowe oraz je skonfiguruje
- skonfiguruje wszystkie posiadane VPN oraz doda nowe zgodnie z przekazaną listą Zamawiającego
- potwierdzi działanie sieci, urządzeń i wszystkich systemów po zakończonej konfiguracji

Zamawiający informuje iż posiada łącza ministerialne którymi nie zarządza, Wykonawca musi skonfigurować na dostarczanym urządzeniu łącza ministerialne w sposób zachowujący ciągłość działania urzędu.

b) Dostawa instalacja i konfiguracja systemu do wirtualizacji, utworzenie dwóch maszyn wirtualnych

W ramach zadania Wykonawca dostarczy zainstaluje i skonfiguruje system do wirtualizacji spełniający minimalne wymagania:

- Licencja producenta na oprogramowanie do wirtualizacji dla minimum 3 serwerów fizycznych bez limitu na ilość rdzeni wraz z licencją na oprogramowanie do centralnego zarzadzania klastrem serwerów
- Wykonawca dostarczy, zainstaluje, skonfiguruje oraz przeniesienie na zamawiającego własność licencji na oprogramowanie do wirtualizacji wraz z wsparciem na kres 36 miesięcy
- Warstwa wirtualizacji musi być instalowana bezpośrednio na sprzęcie fizycznym bez potrzeby instalowania dodatkowego systemu operacyjnego.
- Oprogramowanie musi umożliwiać budowanie klastrów wysokiej dostępności.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i musi się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
- Oprogramowanie do wirtualizacji umożliwiać przenoszenie maszyn wirtualnych bez konieczności ich wyłączania
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do min 4TB pamięci operacyjnej.
- Oprogramowanie do wirtualizacji musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych, niż fizyczne zasoby RAM serwera, w celu osiągniecia konsolidacji.
- Oprogramowanie do wirtualizacji musi być niezależne od producenta platformy sprzętowej.

- Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich sprawnego odtwarzania.

W ramach zadania Wykonawca zainstaluje dwie maszyny wirtualne wg. Wytycznych Zamawiającego na wskazanym przez Zamawiającego serwerze fizycznym.

c) Migracja posiadanych serwerów na maszyny wirtualne

W ramach zadania wykonawca wykona migrację dwóch serwerów opartych o Windows 2019 Server na maszyny wirtualne. Przed wykonaniem Wykonawca wykona backup migrowanych serwerów oraz potwierdzi możliwość jego przywrócenia w razie błędnego działania migrowanej maszyny. Po dokonaniu migracji Wykonawca zweryfikuje i potwierdzi poprawność działania systemów działających na zmigrowanych serwerach.

d) Przeprowadzenie szkoleń dla personelu Zamawiającego w zakresie administrowania i użytkowania wdrażanych rozwiązań, oraz wsparcie serwisowe

Wykonawca zobligowany jest do przeprowadzenia szkolenia z zakresu wdrażanych rozwiązań. Szkolenie będzie realizowane w formie stacjonarnej, w siedzibie Zamawiającego. Dodatkowo Wykonawca zapewni wsparcie serwisowe Zamawiającego w zakresie wdrożonych rozwiązań wilości 4 godzin online do wykorzystania w dowolnym czasie.

UWAGA:

Wszystkie prace wykonywane w ramach zamówienia nie mogą wpłynąć na negatywnie na ciągłość działania Urzędu. Zamawiający wymaga zatem aby wszystkie prace wykonywane były poza godzinami pracy Urzędu.