Główny Inspektorat
Ochrony Środowiska

Załącznik nr 1 - Opis Przedmiotu Zamówienia

„Zakup urządzeń brzegowych oraz dodatkowego rozwiązania ochrony poczty”

1. Skrócony opis zamówienia

Zamówienie składać się będzie z dostarczenia do siedziby GIOŚ, ul. Bitwy Warszawskiej 1920 r. 3 w Warszawie wyspecyfikowanych urządzeń, licencji, konfiguracji, instalacji oraz zapewnienie usług gwarancyjnych w tym zakresie.
Zakłada się, że zamówienie będzie podzielone na II niezależne części, szacunkowe oferty dla każdej części będą rozpatrywane osobno.
Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony Wykonawcy wymaga się w II części zamówienia, aby wszystkie funkcje oraz zastosowane technologie pochodziły od jednego producenta.

2. Szczegółowy opis zamówienia

Konfiguracja i instalacja komponentów zostanie wykonana przez Wykonawcę, wliczając produkcyjne uruchomienie systemu z zabezpieczeniem ochrony usług Microsoft Exchange 2019 z części II zamówienia.

Wykonawca zapewni również 30 godzin asysty technicznej w okresie pierwszych 12 miesięcy od uruchomienia i wdrożenia urządzeń i oprogramowania, świadczonej zdalnie lub w siedzibie Zamawiającego. Po wdrożeniu Wykonawca przekaże Zamawiającemu dokumentację techniczną wdrożonych rozwiązań.

Systemy muszą być objęte serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia/oprogramowania w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

I część Zamówienia:

2x zapora sieciowa ze wsparciem i serwisami bezpieczeństwa

Przedmiot zamówienia obejmuje zwiększenie obecnej infrastruktury w celu ochrony przed zagrożeniami, musi umożliwiać integrację z rozwiązaniami typu FortiGate, w zakresie logowania, budowy topologii sieci oraz integracji z systemem FortiAnalyzer w zakresie rejestrowania, kolekcjonowania, monitorowania, przetwarzania i analizowania danych w zakresie bezpieczeństwa oraz integrację z FortiManager w zakresie zarządzania.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione w niniejszym dokumencie funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Urządzenia o tym samym modelu docelowo muszą być skonfigurowane w układzie klastra.

Dostarczony sprzęt musi być fabrycznie nowy i pochodzić z oficjalnej dystrybucji na Polskę.

System musi wspierać IPv4 oraz IPv6 w zakresie:

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

Wykonawca zobowiązany będzie dostarczone urządzenia zamontować w szafie rack 19". Wraz z urządzeniami wykonawca dostarczy i zamontuje wszystkie niezbędne elementy do montażu i połączeń sieciowych (np.: wkładki SFP , patchcordy, elementy montażowe) w szafie rack 19".

Za pomocą dostarczonych urządzeń musi być możliwość zbudowania klastra HA - Active-Active lub Active-Passive.

System realizujący funkcję Firewall musi dysponować minimum:

- 1x GE RJ45 HA / MGMT Ports
- 16x GE RJ45 Ports
- 4x 10 GE SFP+ Slots
- IPS Throughput : 5 Gbps
- NGFW Throughput: 3.5 Gbps
- Threat Protection Throughput: 3 Gbps
- IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP): 27 / 27 / 11 Gbps
- Firewall Latency (64 byte, UDP): 4.78 µs
- Firewall Throughput (Packet per Second): 16.5 Mpps
- Concurrent Sessions (TCP): 3 Million
- New Sessions/Second (TCP): 280 000
- Firewall Policies: 10 000
- IPsec VPN Throughput (512 byte): 13 Gbps
- Gateway-to-Gateway IPsec VPN Tunnels: 2000
- Client-to-Gateway IPsec VPN Tunnels: 16 000
- SSL-VPN Throughput: 2 Gbps
- Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode): 500
- SSL Inspection Throughput (IPS, avg. HTTPS): 4 Gbps
- SSL Inspection CPS (IPS, avg. HTTPS): 3500
- SSL Inspection Concurrent Session (IPS, avg. HTTPS): 300 000
- Application Control Throughput (HTTP 64K): 13 Gbps
- CAPWAP Throughput (HTTP 64K): 20 Gbps
- Virtual Domains: 10
- High Availability Configurations: Active-Active, Active-Passive, Clustering

System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

Urządzenie musi zapewnić obsługę i integrację z posiadającymi przez Zamawiającego urządzeniami typu Access Point Fortinet AP 221E, FortiSwitch 148E, 124E oraz 124E-POE;

System musi być wyposażony w dwa redundantne zasilacze AC

Licencje, dostarczone wraz z urządzeniami muszą upoważniać do korzystania z aktualnych baz producenta i serwisów:

- 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.

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.

Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje:

- 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).
- Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
- Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania muszą 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.
- Analiza ruchu szyfrowanego protokołem SSL.
- Analiza ruchu szyfrowanego protokołem SSH.

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.

W zakresie routingu rozwiązanie powinno zapewniać obsługę:

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

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

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.

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.

A. Zapora musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
B. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
C. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
D. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 4321).
E. System musi umożliwiać skanowanie archiwów, w tym co najmniej: ZIP.
F. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
G. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
H. Ochrona przed atakami na aplikacje pracujące na niestandardowych portach.
I. Baza sygnatur ataków powinna zawierać minimum 10000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
J. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
K. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
L. 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.
M. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
N. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
O. Baza Kontroli Aplikacji powinna zawierać minimum 4000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
P. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
Q. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
R. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
S. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 60 milionów adresów URL pogrupowanych w kategorie tematyczne.
T. W ramach filtra www muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.
U. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

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

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.

Y. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
Z. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
AA. 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.
BB. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
CC. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
DD. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
EE. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

II część Zamówienia:

a) 1x Oprogramowanie do ochrony poczty z wsparciem i serwisami bezpieczeństwa

Przedmiot obejmuje rozbudowę obecnej infrastruktury Fortinet poprzez dostawę oprogramowania do ochrony poczty wraz ze wsparciem technicznym i serwisami bezpieczeństwa. Oprogramowanie musi umożliwiać integrację z rozwiązaniami typu FortiGate, w zakresie logowania, budowy topologii sieci oraz integracji z systemem FortiAnalyzer w zakresie rejestrowania, kolekcjonowania, monitorowania, przetwarzania i analizowania danych w zakresie bezpieczeństwa.

Dostarczony system ochrony poczty musi zapewniać poniższe funkcje:

- logowanie do zewnętrznego serwera SYSLOG;
- logowanie zmian konfiguracji oraz zdarzeń systemowych;
- logowanie informacji na temat spamu oraz niedozwolonych załączników;
- możliwość podglądu logów w czasie rzeczywistym;
- powiadomienie administratora systemu w przypadku wykrycia zagrożeń bezpieczeństwa poczty;
- możliwość generowania raportów zgodnie z harmonogramem lub na żądanie;
- wsparcie dla co najmniej 100 domen pocztowych;
- polityki filtrowania poczty tworzone co najmniej w oparciu o adresy mailowe, nazwy domenowe, adresy ip;
- routing email w oparciu o reguły lub o zewnętrzny serwer LDAP;
- zarządzanie kolejkami wiadomości;
- ochrona i analiza poczty przychodzącej i wychodzącej;
- szczegółowe, wielowarstwowe polityki wykrywania spamu, wirusów;
- możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP;
- kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania wiadomości z kwarantanny użytkownika;
- dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz Pop3;
- archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki;
- backup poczty realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach;
- białe i czarne listy adresów mailowych definiowanych globalnie oraz dla domen wskazanych przez administratora systemu;
- białe i czarne listy adresów mailowych dla użytkowników;
- zapobieganie przed wyciekiem informacji poufnej DLP;
- skanowanie antywirusowe wiadomości SMTP;
- kwarantanna dla zainfekowanych plików;
- skanowanie załączników skompresowanych;
- definiowanie komunikatów powiadomień w języku polskim;
- blokowanie załączników w oparciu o typ pliku;
- możliwość zdefiniowania nie mniej niż [50] polityk kontroli antywirusowej;
- moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu;
- reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta;
- filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania;
- szczegółowa kontrola nagłówka wiadomości;
- analiza heurystyczna;

- współpraca z zewnętrznymi serwerami RBL, SURBL;
- filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen;
- możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników;
- wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF;
- kontrola w oparciu o Greylisting oraz SPF;
- filtrowanie treści wiadomości i załączników;
- kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości;
- możliwość zdefiniowania nie mniej niż [50] polityk kontroli antyspamowej;
- ochrona typu outbreak;
- filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking);
- system musi realizować skanowanie antyspamowe z wydajnością min. 54 tys. wiadomości/godzinę;
- definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej tagowanie wiadomości.

b) 1x Oprogramowanie do Autentykacji 2FA dla 1300 użytkowników z wsparciem i serwisami bezpieczeństwa

Przedmiot umożliwia stosowanie zasad bezpieczeństwa opartych na rolach oraz tożsamościach w zabezpieczonej sieci Fortinet dla 1300 użytkowników. Zwiększenie bezpieczeństwa poprzez centralizację zarządzania i przechowywania wykorzystywanych podczas uwierzytelniania informacji o użytkownikach. Dostarczony system uwierzytelniania musi zapewniać wszystkie wymienione poniżej funkcje.

Dostarczony system ochrony musi zapewniać poniższe funkcje:

- wsparcie dla minimum 4 interfejsów sieciowych. Obsługa powierzchni dyskowej - minimum 200 GB;

System powinien pozwalać na nie mniej niż:

- zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki, bez konieczności stosowania zewnętrznej konsoli zarządzającej;
- możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active -Active w celu zwiększenia niezawodności;
- odpytywanie o stan urządzenia w oparciu o protokół SNMP (v1, v2, v3) oraz wykorzystanie SNMP Trap celem monitorowania (nie mniej niż):
  - obciążenia procesor(a/ów);
  - wykorzystania pamięci;
  - informacji o osiąganiu granicznej liczby użytkowników;
  - informacji o osiąganiu granicznej liczby grup użytkowników;
  - informacji o osiąganiu granicznej liczby uwierzytelnionych użytkowników;
  - przekroczeniu ilości uwierzytelnień;
  - przekroczeniu ilości błędnych uwierzytelnień;
- graficzną reprezentację statusu uwierzytelnień;
- logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia i nazwy użytkownika:

        - lokalnie;
        - zdalnie w oparciu o protokół syslog;
    - aktualizację systemu operacyjnego z poziomu graficznego interfejsu zarządzającego (GUI);
    - tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI):
        - również w oparciu o harmonogram w cyklu godzinowym, dziennym, tygodniowym lub miesięcznym wraz z określeniem godzin i minut
        - rzeczona kopia bezpieczeństwa może również być również zapisywana przy pomocy protokołu FTP/SFTP;
    - konfigurację captive portal;

  Celem realizacji funkcji uwierzytelniających, system powinien wspierać nie mniej niż:

    - lokalną, wbudowaną bazę użytkowników wraz z możliwością wykonywania nie mniej niż następujących akcji na użytkowniku: tworzenie, przypisanie tokenu oraz zarządzanie nim, blokowanie konta (locking), usuwanie;
    - przechowywanie następujących informacji o użytkowniku: nazwa (username), imię/nazwisko, adres email, numer telefonu komórkowego, numer telefonu, adres, kraj, stan/województwo;
    - możliwość przechowywania przynajmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników;
    - możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV;
    - konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:
        - poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych);
        - czasu życia hasła;
        - możliwości ponownego użycia tych samych haseł;
    - konfigurowalną politykę blokowania kont:
        - w oparciu o ilość nieudanych logowań;
        - czas blokowania;
        - okres nieaktywności po którym konto jest blokowane;
    - możliwość odzyskiwania haseł:
        - z wykorzystaniem adresu email;
        - z wykorzystaniem pytania pomocniczego;

- uruchomienie portalu do samodzielnej rejestracji użytkowników
- opcjonalnie tworzenie ich kont może wymagać akceptacji administratora
- wymagana jest również opcja tworzenie kont bez ingerencji administratora
- obsługę protokołu RADIUS zgodną z RFC
- wbudowany serwer RADIUS
- konfiguracja serwera pozwala na ograniczenie dostępu tylko do wskazanych urządzeń NAS
- integrację z zewnętrznymi serwerami RADIUS
- obsługę protokołu LDAP
- wbudowny serwer LDAP

- możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP)
- obsługę SAML
- realizacje funkcjonalności SSO (Single Sign On) w oparciu o:
- integrację z Active Directory również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny
    - dedykowaną aplikację na stację robocze z systemem Windows
    - RADIUS
    - informacje uzyskiwane poprzez protokół syslog
    - dedykowany portal
- Realizując uwierzytelnianie dwuskładnikowe, system musi spełniać nie mniej niż:
    - obsługę dla tokenów sprzętowych (hardware):
    - ich działanie musi być realizowane w oparciu o protokół OATH wraz ze wsparciem dla TOTP oraz HOTP;
    - wspomniane tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania;
- wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile;
- dla tokenów na system iOS i Android wymaga się:
    - aktywacji z centralnego systemu uwierzytelniania (seed provisioning);
    - możliwości konfiguracji ilości generowanych cyfr (6 lub 8);
    - generowania kodu (cyfr) co 30 lub 60 sekund;
    - możliwości dezaktywacji tokena oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne);
    - ochrony dostępu poprzez konfigurowalny kod PIN;
    - aktywacji w oparciu o kod QR;
- możliwość dostarczenia kodu (wskazania tokena) poprzez:
    - email (wygaśnięcie kodu w czasie 10-3600 sekund);
    - SMS (wygaśnięcie kodu w czasie 10-3600 sekund);
        - konfiguracja bramki SMS w oparciu o HTTP/S i/lub SMTP.
- w przypadku tokenów programowych możliwość wykorzystania notyfikacji push przychodzących na urządzenie mobilne i zawierających szczegóły dotyczące żądania logowania (nazwa użytkownika, serwer/usługa docelowa, adres IP, data i godzina, rodzaj i wersja przeglądarki) w celu zaakceptowania ich jednym "kliknięciem";
- możliwość integracji z logowaniem do systemu Windows;
- wsparcie dla API.

System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protkołu 802.1x, spełniając nie mniej niż następujące warunki:

- dla sieci bezprzewodowych wymagane są następujące protokoły:
    - PEAP
    - EAP-TTLS

    - EAP-TLS
    - EAP-GTC
- wsparcie dla uwierzytelniania w oparciu o adres MAC (MAC based authentication);
- zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTL, TLS EAP;
- możliwość samodzielnej rejestracji urządzeń przez użytkowników celem uwierzytelniania z wykorzystaniem certyfikatów;

System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż:

- własne, samodzielne CA (Certificate Authority);
- CA pośredniczące (intermediary CA);
- ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego;
- możliwość pobrania wygenerowanych certyfikatów;
- możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP;
- możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP;
- możliwość generowania certyfikatów typu wildcard;
- realizacja CRL (Certificate Revocation List);
- wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560);

Urządzenie musi obsługiwać co najmniej:

- uwierzytelnianie dla 1300 użytkowników
- 1300 tokenów (uwierzytelnianie dwuskładnikowe)
- 1300 klientów protokołu RADIUS (urządzeń NAS)

System udostępnia:

- Graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS

Wymaga się aby dostawa obejmowała również:

- Gwarancję i serwis producenta na okres 36 miesięcy;
- lokalny magazyn: dysk twardy 2x 1 TB;
- liczba użytkowników lokalnych/zdalnych: 1500/3500;
- wirtualne procesory: maksymalnie 64;
- pamięć wirtualna: 2 GB/1 TB;
- interfejs wirtualny: minimalny 1/maksymalny 4;
- uwierzytelnianie użytkowników z wykorzystaniem standardowych mechanizmów RADIUS lub LDAP;
- integracja technologii jednokrotnego logowania FSSO z istniejącą infrastrukturą Active Directory;
- możliwość stosowania polityki FortiGate opartej na tożsamościach użytkowników;
- lokalny interfejs oparty na sieci Web;
- integracja z istniejącymi bazami danych uwierzytelniających opartymi na LDAP;
- uwierzytelnienie dwuskładnikowe;
- interfejs zarządzania z poziomu wiersza poleceń (ang. Command Line Management Interface, CLI);
- kontrola dostępów do portów 801.1x oraz zarządzanie certyfikatami;

- wykrywanie zmiany adresu IP, zabezpieczenie infrastruktury sieciowej;
- zarządzanie certyfikatami na potrzeby wdrażania sieci bezprzewodowych i VPN;
- kompatybilność oraz integracja z oferowanym rozwiązaniem z oprogramowaniem do ochrony Exchange Outlook Web App.

c) 1x Oprogramowanie do ochrony Exchange Outlook Web App ze wsparciem i serwisami bezpieczeństwa

Przedmiot Zamówienia obejmuje środowisko do ochrony Exchange OWA ze wsparciem i serwisami bezpieczeństwa, którego zadaniem będzie wykrywanie oraz blokowanie ataków. Powinna istnieć możliwość zdefiniowania co najmniej 4 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu. Nie powinno być ograniczeń chronionych aplikacji web.

Dostarczony system ochrony musi zapewniać poniższe funkcje:

- terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla SSL 3.0, TLS 1.1, TLS 1.2;
- możliwość analizy poszczególnych rodzajów ruchu w oparciu o polityki bezpieczeństwa;
- kontrola komunikacji XML z możliwością routingu w oparciu o kontent, walidacją schematu XML;
- mechanizmy ochrony przed wyciekiem informacji poufnych;
- analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania;
- możliwość selektywnego wyłączania blokowania ataków dla sygnatur oraz obszarów aplikacji. Wyłączanie konkretnych sygnatur na podstawie wielu parametrów: profil bezpieczeństwa (m.in. IP, metoda HTTP, cookie);
- rozpoznawanie użytkowników logujących się bezpośrednio do chronionej aplikacji bez udziału WAF;
- wsparcie dla CAPTCHA do weryfikacji użytkowników;
- dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, API;
- możliwość konfigurowania własnych stron z informacjami o błędzie;
- wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej;
- ustawienie wymaganej sekwencji otwieranych stron;
- budowa rankingu punktowego lub określanie poziomu zagrożenia dla ruchu od użytkowników generujących ataki z możliwością określenia progów dla poszczególnych akcji: logowanie, blokowanie, kwarantanna czasowa;
- system musi zapewniać lokalne logowanie oraz raportowanie - w oparciu o zestaw predefiniowanych wzorców raportów;
- obsługa awaryjności powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa mailem.