Dostawa urządzenia Firewall wraz z oprogramowaniem (1 szt.).
Minimalne parametry techniczne i funkcjonalne:

1. Elementy systemu bezpieczeństwa:
   a. Urządzenie musi mieć możliwość pracy w trybie Layer 3 (routing) oraz Layer 2(bridge)
   b. Możliwość stworzenia minimum 128 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q.
   c. W zakresie Firewall, obsługa nie mniej niż 2 200 000 jednoczesnych połączeń i 130 000 nowych połączeń na sekundę.
   d. System realizujący funkcję Firewall musi być wyposażony lub musi mieć możliwość rozbudowy o dysk o minimalnej pojemności 512 GB do celów logowania i raportowania.
   e. Musi posiadać 2x USB 3.0 z przodu urządzenia
   f. Musi posiadać 1x port konsoli
   g. System musi posiadać system raportowania i przeglądania logów. Moduł może być dostarczony w postaci osobnej, komercyjnej instancji fizycznej lub wirtualnej, pochodzącej od tego samego producenta co system Firewall.
   h. System pełniący funkcję zapory musi posiadać nie mniej niż: 8xSFP+, 8x SFP, 8x GE interfejsów.
   i. System musi posiadać możliwość wykorzystania portu USB jako Modemu WAN 4G lub dodatkowego dysku na dane
   j. System musi posiadać zewnętrzy przycisk, pozwalając na reset urządzenia do ustawień fabrycznych, bez konieczności logowania się do urządzenia
   k. Urządzenie musi być wyposażone w wbudowane, redundantne zasilanie

2. Funkcjonalności:
   a. Kontrola dostępu — zapora sieciowa Stateful Inspection
   b. Ochrona przed wirusami - komercyjny antywirus [AV]
   c. Poufność danych - IPSec VPN i SSL VPN
   d. Kontrola witryn sieci Web — filtr URL
   e. Kontrola zawartości poczty - antyspam (dla protokołów SMTP, POP3)
   f. Kontrola przepustowości i ruchu [QoS i kształtowanie ruchu] z alokacją Tunnel w oparciu o strefę bezpieczeństwa, interfejs, adres, użytkownika/grupę użytkowników, serwera/ grupę serwerów, aplikację/grupę aplikacji, TOS, VLAN
   g. Kontrola aplikacji i rozpoznawanie ruchu P2P (wideo, gry itp.)
   h. Reputacja IP
   i. Cloud Sandbox
   j. API – możliwość wgrywania i wyciągania informacji z systemu dedykowanym interfejsem Rest API

3. Wydajność:
   a. Analiza ruchu szyfrowanego protokołem SSL
   b. Wydajność Firewall co najmniej 10 Gb/s
   c. Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym IPS i kontrolą aplikacji 4.5 Gb/s
   d. Wydajność ochrony przed atakami (IPS) minimum 9 Gb/s
   e. Wydajność AV nie mniej niż 4.5 Gb/s
   f. Wydajność skanowania z włączoną kontrolą aplikacji, AV, IPS, filtrem URL nie mniejsza niż 2.5 Gb/s

4. Funkcjonalności VPN:
   a. Wydajność IPSec VPN, nie mniej niż 5.2 Gb/s
   b. Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja
   c. Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem przynajmniej na Mac i Windows
   d. Monitorowanie stanu tuneli VPN i utrzymywanie ich aktywności
   e. Praca w toplogiach Hub and Spoke i Mesh
   f. Wspierane mechanizamy : IPSec NAT Traversal, DPD, Replay Detection, Xauth, DHCP over IPsec,
   g. Wsparcie grup DH dla IKEv1: 1,2,5,19,20,21
   h. Wsparcie grup DH dla IKEv2: 1,2,5,14,15,19,20,21
   i. Możliwość rozszerzania ilości użytkowników VPN odpowiednią licencją lub nielimitowana ilość użytkowników SSL VPN
   j. Możliwość korzystania z NAT 1-1 w tunelu VPN

5. Routing:
   a. Rozwiązanie musi zapewniać: obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP
   b. Obsługa Policy Based Routing

6. Translacja adresów NAT:
   a. Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego.

7. Polityka bezpieczeństwa systemu:
   a. Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników i grupy użytkowników, reakcje bezpieczeństwa, rejestrowanie zdarzeń i zarządzanie pasmem sieci (w tym gwarantowaną i maksymalną przepustowość, priorytety).
   b. Możliwość budowania min. 12000 polityk
   c. Musi posiadać funkcjonalność asystenta polityk
   d. Musi być w stanie skonfigurować agregowane polityki
   e. Musi być w stanie ograniczyć pasmo na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu

8. Wydzielenie stref bezpieczeństwa:
   a. Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN

9. Ochrona antywirusowa:
   a. Silnik antywirusowy musi być oparty na przepływie tzw. flow-based
   b. Musi umożliwiać skanowanie protokołów HTTP, SMTP, POP3, IMAP, FTP / SFTP
   c. Możliwość ręcznego dodawania lub usuwania sygnatury MD5 do bazy danych AV
   d. Musi obsługiwać wykrywanie wirusów w plikach skompresowanych, takich jak RAR, ZIP, GZIP, TAR, a także wykrywać zaszyfrowane/zahasłowane pliki

10. Równoważenie obciążenia:
    a. Obsługa redundantnego równoważenia obciążenia serwerów
    b. Obsługa równoważenia obciążenia serwerów w oparciu o weighted round-robin
    c. Monitorowanie sesji i ochrona sesji

11. Ochrona IPS:
    a. Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury.

b. Baza danych wykrytych ataków musi zawierać co najmniej 8000 sygnatur. Dodatkowo musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i Ddos.
c. Funkcjonalność zapobiegania atakom SQL injection, XSS injection

12. Obrona przed atakiem:
    a. Ochrona przed nieprawidłowym działaniem protokołu
    b. Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, TCP fragment, ICMP fragment itp.
    c. Biała lista adresów IP

13. Ochrona antyspam
    a. Rozwiązanie musi zapewniać ochronę przed spamem w czasie rzeczywistym
    b. Wspieranymi protokołami są minimum SMTP, SMTPS, POP3, POP3S
    c. Skanowanie antyspamowe musi odbywać się w ruchu w obu kierunkach
    d. Musi istnieć możliwość dodawania wyjątków w zakresie skanowania antyspamowego, minimum białych list domen

14. Kontrola aplikacji:
    a. Kontrola aplikacji musi być w stanie kontrolować ruch w oparciu o głęboką analizę pakietów, a nie tylko w oparciu o wartości portów TCP/UDP
    b. Baza danych aplikacji zawierająca ponad 1800 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka

15. Filtr adresów URL:
    a. Baza filtrów URL pogrupowana w co najmniej 64 kategorie tematyczne.
    b. Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL.
    c. Kategoria takie jak hazard, malware, spam, botnety
    d. Obsługa Safe Search
    e. Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne
    f. Dostosowanie strony ostrzeżenia

16. Reputacja IP:
    a. Identyfikacja i filtrowanie ruchu z ryzykownych adresów IP, takich jak hosty botnet, spamerzy, węzły Tor, podejrzane hosty i adresy IP atakujące metodą brute force
    b. Logowanie, odrzucanie pakietów lub blokowanie dla różnych rodzajów ryzykownego ruchu IP

17. Zapobieganie botnetom:
    a. Wykrywanie intranetowych hostów botnetu, monitorując połączenia C&C i blokowanie dalszych zaawansowanych zagrożeń takich jak botnet i oprogramowanie ransomware
    b. Wsparcie DNS sinkhole

18. Cloud Sandbox:
    a. Złośliwe oprogramowanie emulowane w wirtualnym środowisku oparte na architekturze chmury w celu wykrywania nieznanych zagrożeń
    b. Obsługa protokołów, takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP
    c. Obsługa typów plików : PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów

19. Uwierzytelnianie użytkownika:
    a. System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika z nie mniej niż:
    i. Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu
    ii. Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP
    iii. Hasła dynamiczne (RADIUS) oparte o zewnętrzne bazach danych
    b. Musi umożliwiać budowę architektury uwierzytelniania pojedynczego logowania w środowisku Active Directory
    c. Wsparcie usług terminalowych
    d. Uwierzytelnianie użytkownika przez Web przed dostępem do internetu
    e. System musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania

20. Raportowanie i przeglądanie logów:
    a. System raportowania i przeglądania logów musi zostać dostarczony na ten sam okres, co wsparcie oraz subskrypcja na system Firewall
    b. W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż:
    i. Posiadanie predefiniowanych raportów/dashboardów dla ruchu internetowego, modułu IPS, skanera antywirusowego i antyspamowego czy uwierzytelnionych użytkowników
    ii. Generowanie co najmniej 20 rodzajów raportów/dashboardów

21. Wysoka dostępność:
    a. Rozwiązanie musi obsługiwać tryby Active/Active i Active/Passive
    b. Rozwiązanie musi obsługiwać następujące opcje wdrażania HA:
    i. HA z agregacją linków
    ii. Geograficznie rozproszony HA

22. System logowania:
    a. Wraz z systemem musi być zapewniony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy chmurowej, do której dostęp jest cały czas z dowolnego urządzenia oraz dedykowanej aplikacji mobilnej.

23. Certyfikaty - Rozwiązanie musi:
    a. posiadać certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSA Labs dla funkcji Firewall
    b. być pozycjonowanym w raporcie Gartnera przez ostatnie 8 lat

24. Zarządzanie:
    a. Elementy systemu muszą mieć możliwość zarządzania lokalnie (HTTPS, SSH) oraz współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja między systemami bezpieczeństwa a platformami zarządzania musi odbywać się za pomocą protokołów szyfrowanych.
    b. Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI lub po pomocą linuii komend (COM Port, SSH) bez instalowania oddzielnego oprogramowania, takiego jak dedykowana aplikacja

25. Gwarancja – Dostawa musi zawierać również:
    a. 48-miesięczną gwarancję producenta na dostarczone elementy systemu
    b. Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 48 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)

c. Wsparcie techniczne dystrybutora rozwiązań w języku polskim
d. Oferta musi być złożona przez autoryzowanego partnera