Załącznik nr 3 – opis przedmiotu zamówienia

Wymagania ogólne w zakresie dostawy sprzętu.

1. Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt musi być fabrycznie nowy (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale" oraz „end-of-support" producenta.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Dostarczone rozwiązania musi być połączone z wdrożeniem w siedzibie Zamawiającego, dostosowane do zapotrzebowania i infrastruktury Zamawiającego. Instalacja i wdrożenie powinno odbywać się stacjonarnie w siedzibie Zamawiającego. Szkolenie dla administratorów. Wymagane jest przeszkolenie co najmniej dwóch administratorów wskazanych przez Zamawiającego. Szkolenie musi odbywać się stacjonarnie w siedzibie Zamawiającego. Minimalny czas trwania szkolenia to 8 godzin zegarowych

I. <u>Dostawa urządzenia klasy NDR wraz z oprogramowaniem (1 szt.).</u>

Minimalne parametry techniczne i funkcjonalne:

1. Elementy systemu bezpieczeństwa
   a. Wysokość 1U do montażu w szafie rack.
   b. Posiadać co najmniej dwa porty USB
   c. Urządzenie musi posiadać dedykowany port do zarządzania
   d. Urządzenie musi posiadać minimum interfejsów: 2x SFP+, 8x SFP, 8x GE
   e. Musi obsługiwać co najmniej 1T przestrzeni dyskowej.
   f. Minimum 1 Gb/s przepustowości wykrywania naruszeń w dwukierunkowym ruchu HTTP z włączonymi wszystkimi funkcjami wykrywania zagrożeń
   g. Proponowane rozwiązanie musi obsługiwać minimum 750 tys . jednoczesnych sesji.
   h. Proponowane rozwiązanie musi obsługiwać 32000 nowych sesji /s w ruchu HTTP.
2. Usługi sieciowe
   a. Musi obsługiwać pasywny tryb pracy (TAP), nie ingerując w sieć klienta.
   b. Rozwiązanie musi być w stanie zintegrować się z zaporami ogniowymi tej samej marki w celu ograniczenia zagrożeń
   c. Musi posiadać możliwość rozwiązywania wiadomości przez protokół MPLS, VXLAN oraz QinQ i wykrywania zagrożeń w tych wiadomościach.
3. Kontrola aplikacji
   a. Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka oraz wspierać komunikatory internetowe, p2p, pocztę e-mail, przesyłanie plików, gry online, strumieniowe przesyłanie multimediów itp.
   b. Rozwiązanie musi być w stanie zidentyfikować aplikacje mobilne typu iOS lub Android.
   c. Rozwiązanie musi być w stanie identyfikować aplikacje w chmurze, musi zapewniać wielowymiarowe monitorowanie i statystyki dla aplikacji w chmurze, w tym kategorię ryzyka i funkcje.
4. Wykrywanie zagrożeń
   a. Rozwiązanie musi obsługiwać co najmniej 30000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, ręczne i automatyczne aktualizacje, wyodrębnianie sygnatur oraz wbudowaną encyklopedię zagrożeń.
   b. Rozwiązanie musi obsługiwać ochronę przed atakami SQL injection, XSS, buffer overflow zarówno

dla IPv4 jak i IPv6
c. Rozwiązanie powinno obsługiwać ochronę przez atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, Musi obsługiwać wykrywanie co najmniej metod uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA
d. Rozwiązanie musi obsługiwać wykrywanie anomalii protokołów HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS itp.
e. Niestandardowe reguły wykrywania włamań muszą obsługiwać konfigurowanie kierunku ruchu ataku w celu poprawy dokładności analizy źródła ataku.
f. Rozwiązanie powinno umożliwiać tworzenie białych list dla modułu IPS.
g. Rozwiązanie musi mieć wstępnie zdefiniowane profile IPS.
h. Rozwiązanie musi mieć opcję przechwytywania pakietów
i. Rozwiązanie musi umieć wykrywa reverse-shell
j. Rozwiązanie potrafi zdefiniować odpowiednie treshholdy chroniące przed atakami Flood, bazując na parametrach dostarczonego ruchu
k. System musi mapować wykryte zagrożenia na framework MITRE ATT&CK

5. Skanowanie antywirusowe
   a. Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur.
   b. Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP.
   c. Rozwiązanie powinno obsługiwać wykrywanie wirusów w skompresowanych plikach, takich jak RAR, ZIP, GZIP, BZIP2, TAR oraz wspierać wielowarstwowe wykrywanie skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji po wykryciu zagrożenia w tych plikach
   d. Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików
6. Wykrywanie botnetów C&C
   a. Rozwiązanie powinno wspierać skuteczne wykrywanie botów intranetowych i zapobieganie dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównywanie uzyskanych informacji z bazą adresów C&C.
   b. Rozwiązanie musi obsługiwać automatyczną aktualizację sygnatur botnetów C&C
   c. Rozwiązanie musi obsługiwać dwa typy bazy adresów C&C: bazę adresów IP i bazę danych domen.
   d. Rozwiązanie musi obsługiwać wykrywanie C&C protokołów w protokołach TCP, HTTP i DNS.
   e. Rozwiązanie musi wspierać właczenie wykrywania DGA w celu analizy odpowiedzi DNS i wykrywania, czy urządzenie jest atakowane przez nazwę domeny DGA.
   f. Musi wspierać wykrywanie tunelowania w protokole DNS w tym analizowanie zapytań DNS a także rejestrować logów zagrożeń wykrytych tuneli DNS.
7. Sandbox w chmurze
   a. Rozwiązanie musi obsługiwać oparte na chmurze wirtualne środowisko analizy złośliwego oprogramowania w celu znalezienia nieznanych zagrożeń
   b. Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do piaskownicy w chmurze w celu analizy.
   c. Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów, w tym HTTP/HTTPS, POP3, IMAP4, SMTP i FTP.
   d. Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR , SWF oraz skrypty
   e. Rozwiązanie powinno dostarczyć kompletny raport analizy behawioralnej dla złośliwych plików.
   f. Rozwiązanie musi obsługiwać globalne udostępnianie informacji o zagrożeniach, aby wykryć nowe nieznane zagrożenie.
8. Wykrywanie spamu
   a. Rozwiązanie musi wspierać klasyfikację i wykrywanie spamu w czasie rzeczywistym
   b. Rozwiązanie musi obsługiwać wykrywanie spamu niezależnie od języka, formatu lub treści wiadomości.

c. Rozwiązanie musi obsługiwać protokoły poczty e-mail smtp i pop3
d. Rozwiązanie musi obsługiwać białe listy wiadomości e-mail z zaufanych domen.

9. Dodatkowe funkcje ochrony
   a. Rozwiązanie musi obsługiwać wykrywanie DoS / DDoS, SYN Flood, DNS query flood itp.
   b. Rozwiązanie musi obsługiwać wykrywanie ataków ARP w tym spoofing ARP
   c. Rozwiązanie musi obsługiwać wykrywanie anormalnych ataków protokołu.
   d. Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu pop
10. Inteligentne funkcje bezpieczeństwa
    a. Rozwiązanie powinno obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowym zachowaniem i zachowaniem aplikacji, aby wykryć potencjalne zagrożenia lub ataki.
    b. Rozwiązanie powinno umożliwiać aktualizację bazy danych modelu zachowania szkodliwego oprogramowania online w czasie rzeczywistym.
    c. Rozwiązanie powinno obsługiwać wykrywanie ponad 2000 znanych i nieznanych rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów itp
    d. Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na obserwacji zachowania
    e. Rozwiązanie musi wspierać wykrycia oprogramowania ransomware i złośliwego oprogramowania do wydobywania kryptowalut.
    f. Rozwiązanie powinno obsługiwać modelowanie zachowania w oparciu o ruch bazowy L3-L7, aby ujawnić nietypowe zachowanie sieci, takie jak skanowanie HTTP, Spider, SPAM, słabe hasła SSH / FTP dla serwerów i hostów.
    g. Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, reflect, dns query, SSL DDos i aplikacyjny DDoS
    h. Rozwiązanie musi obsługiwać inspekcję zaszyfrowanego ruchu tunelowego dla nieznanych aplikacji
    i. Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online w czasie rzeczywistym
    j. Rozwiązanie musi zapewniać analizę kryminalistyczną , w tym analizę zagrożeń, bazę wiedzy, historię i topologię zagrożeń.
    k. Rozwiązanie musi obsługiwać działania administratora w celu zmiany stanu zagrożenia na false positive, naprawionego, zignorowanego, potwierdzonego zdarzenia
    l. Rozwiązanie musi obsługiwać czyszczenie zagrożeń serwera jednym kliknięciem i ponowną ocenę bezpieczeństwa hosta
    m. Rozwiązanie powinno obsługiwać białą listę zagrożeń, w tym nazwę zagrożenia, źródłowy/docelowy adres IP, liczbę odwiedzin itd.
    n. Rozwiązanie musi obsługiwać przechwytywanie pakietów online
    o. Rozwiązanie musi obsługiwać lokalną technologię honeypot, aby wychwytywać ataki zagrożeń sieciowych i potwierdzać źródło zagrożenia, typ zagrożenia i częstość występowania
    p. Rozwiązanie musi obsługiwać wykrywanie oszustw na podstawie behawioralnej dla ftp, HTTP, MYSQL, SSH, TELNET, dokumentów lub baz danych
    q. Rozwiązanie musi obsługiwać funkcję polowania na zagrożenia (threat hunting), aby zebrać kompleksowe dowody i zapewnić dogłębną analizę
    r. Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force remote dekto, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu poprawy wykrywalność funkcji śledzenia zagrożeń.
11. Widoczność ryzyka/zagrożeń
    a. Rozwiązanie musi obsługiwać wizualizację zagrożeń intranetowych dla serwerów (zasobów krytycznych), a także wykrywanie nietypowego ruchu z nimi związanego.
    b. Rozwiązanie musi obsługiwać widoczność zagrożeń dla ryzykownych hostów, w tym nazwy hosta, systemu operacyjnego, przeglądarki, typu usługi, aby rejestrować zagrożenia hosta i nietypowy ruch.
    c. Rozwiązanie musi obsługiwać widoczność podstawowych informacji opartych na hoście, indeksu

ryzyka, zagrożeń i nietypowego ruchu.
d. Rozwiązanie powinno wspierać widoczność zagrożeń, w tym nazwę zagrożenia, typ zagrożenia, poziom ryzyka, bazę wiedzy, pakiet kryminalistyczny itp.
e. Rozwiązanie powinno dostarczyć wszystkie statystyki klasyfikacji zdarzeń zagrożeń w oparciu o IOC i trend zdarzeń zagrożeń w ciągu co najmniej 2 tygodni.
f. Rozwiązanie musi wspierać wskazanie ścieżki ataku.

12. Analiza i odpowiedzi na incydenty
    a. Rozwiązanie musi obsługiwać aktualizację w czasie rzeczywistym najpoważniejszych informacji o zagrożeniach znalezionych w branży do urządzenia z chmury
    b. Obsługa wyświetlania najnowszych informacji o zagrożeniach w wyskakujących okienkach.
    c. Obsługa rejestrowania i sprawdzania, czy w sieci wystąpiło odpowiednie zagrożenie.
    d. Pomoc techniczna w celu dostarczenia szczegółowych informacji o zagrożeniach i sugestii dotyczących rozwiązania.
    e. Wsparcie konfigurowania reguł ostrzegania o zagrożeniach, w tym warunków zagrożenia i metody działania, które w przypadku wystąpienia zdarzenia stanowiącego zagrożenie, system powiadomi użytkownika lub podejmie odpwiedź w odpowiednim czasie zgodnie z metodą działania określoną w regule (np. połączenie z firewall, przypomnienie głosowe lub wysłanie pocztą e-mail.
13. Administracja
    a. Rozwiązanie musi mieć zintegrowany sieciowy interfejs użytkownika (WebUI) i interfejs wiersza poleceń (CLI)
    b. Rozwiązanie powinno obsługiwać zarządzanie dostępem z HTTP/HTTPS, SSH, telnet, konsoli
    c. Rozwiązanie musi być w stanie chronić system przed atakami brute-force na nazwę użytkownika i hasło
    d. Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów.
    e. Rozwiązanie musi obsługiwać monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikując nazwę, system operacyjny, przeglądarkę, typ i rejestr statystyk zagrożeń sieciowych
    f. Oferowany zestaw urządzeń musi pochodzić o jednego producenta i być w pełni kompatybilny
    g. Oferowany zestaw urządzeń musi posiadać aplikację mobilną pozwalającą na monitoring pracy urządzeń i analizę zdarzeń
    h. Rozwiązanie powinno umożliwiać wyświetlanie pełnoekranowe statystyk zagrożeń w czasie rzeczywistym dla serwerów i hostów krytycznych
    i. Dostarczone rozwiązanie powinno zawierać monitor pełnoekranowy 75'' o rozdzielczości minimum 3840x2160, który w czasie rzeczywistym będzie prezentował mapę (geolokalizacę) rozkładu ataków, sytuacji podatności, sytuacji serwerów, sytuacji punktów końcowych, najnowszych zagrożeń, TOP ryzykownych serwerów, TOP ryzykownych punktów końcowych, TOP zagrożeń.
14. Logowanie i raportowanie
    a. Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Raport można wyeksportować co najmniej w formacie PDF i/lub wysłać na adres e-mail lub FTP.
    b. Rozwiązanie powinno obsługiwać ustawianie alarmów dotyczących wykorzystania procesora, wykorzystania pamięci, wykorzystania miejsca na dysku, nowych połączeń itp.
    c. Rozwiązanie powinno obsługiwać wysyłanie alarmów przez e-mail, SMS.
    d. Alerty powinny być generowane na podstawie przepustowości aplikacji i nowych połączeń.
    e. Logi powinny być możliwe do eksportu za pośrednictwem Syslog lub poczty e-mail i zawierać minimum logi zdarzeń, sieci, zagrożenia, konfigurację i sesje
    f. Wstępnie zdefiniowane zadania raportowania
    g. Rozwiązanie powinno mieć scentralizowane monitorowanie wielu urządzeń, w tym procesora, pamięci, ruchu, sesji, aplikacji, użytkowników, zagrożeń itp. za pośrednictwem aplikacji mobilnej z danymi z ostatnich 7 dni.
    h. Rozwiązanie musi wspierać restAPI
15. Gwarancja – Dostawa musi zawierać również
    a. 24-miesięczną gwarancję producenta na dostarczone elementy systemu
    b. Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 24 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
e. Wdrożenie stacjonarne przeprowadzone przez Certyfikowanego inżyniera proponowanego rozwiązania posiadającego certyfikat Professional bądź wyższy.

Monitorowanie zagrożeń w czasie rzeczywistym dla serwerów i hostów krytycznych. Po wykryciu zagrożenia lub nieprawidłowego zachowania przeprowadzi analizę zagrożeń lub zachowań i użyje opartych na topologii prezentacji graficznych, aby zapewnić szeroki wgląd w szczegóły zagrożeń i nieprawidłowości w zachowaniu. Daje to administratorom ds. bezpieczeństwa bezprecedensowy wgląd w postęp ataku, ruch w każdym kierunku, a także ocenę całego ryzyka sieciowego

Dynamiczny, aktualny stan pulpitu nawigacyjnego i widżety do monitorowania zagłębiania się w szczegóły

II. Dostawa urządzenia UTM wraz z oprogramowaniem (2 szt.) – do urzędu.

Minimalne parametry techniczne i funkcjonalne:

1. Elementy systemu bezpieczeństwa:
    a. Urządzenie musi mieć możliwość jednoczesnej pracy w trybie Layer 3 (routing), transparentnym (most) i Layer 2 (port mirroring) bez konieczności wirtualizacji sprzętu
    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 w lokalny dysk o minimalnej pojemności 8 GB do celów logowania i raportowania.
    e. Możliwość rozszerzenia pamięci do 1.92 TB poprzez dodatkowy dysk SSD bez otwierania obudowy urządzenia
    f. Musi posiadać 2x USB 3.0 z przodu urządzenia
    g. System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu.
    h. System musi mieć możliwość włączenia min 1 systemu wirtualnego bez dodatkowej licencji i możliwości rozszerzenia do minimum 5 poprzez dodatkową licencję w przyszłości
    i. Systemy wirtualne muszą obsługiwać QOS
    j. System pełniący funkcję zapory musi posiadać nie mniej niż: 2x SFP+, 8x SFP, 8x GE interfejsów
    k. Urządzenie musi posiadać dedykowany port przeznaczony do zarządzania
    l. System musi posiadać zewnętrzy przycisk, pozwalając na reset urządzenia do ustawień fabrycznych, bez konieczności logowania się do urządzenia
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.) oraz ograniczanie nowych połączeń i jednoczesnych sesji
    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 Gb/s
   d. Wydajność ochrony przed atakami (IPS) minimum 8 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 2.5Gbps.
4. Funkcjonalności VPN:
   a. Wydajność IPSec VPN, nie mniej niż 5 Gb/s
   b. Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja
   c. Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem.
   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: 1,2,5,19,20,21,24
   h. Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,19,20,21,24
   i. Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance) co najmniej w zakresie:
      i. Wersji systemu operacyjnego
      ii. Zaaplikowanych patchy
      iii. Ustawień internetowych
      iv. Zainstalowanego oprogramowania antywirusowego
      v. Włączonego Firewalla
      vi. Walidacji kluczy rejestru
      vii. Walidacji istnienia plików
      viii. Walidacji uruchomionych procesów
      ix. Walidacji uruchomionych lub zainstalowanych serwisów
   j. Możliwość rozszerzania ilości użytkowników VPN odpowiednią licencją
   k. Obsługa PnPVPN (Plug and Play VPN)
5. Routing:
   a. Rozwiązanie musi zapewniać: obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP, IS-IS
   b. Obsługa Policy Based Routing
   c. Funkcjonalność Virtual Wire
6. Translacja adresów NAT:
   a. Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego.
   b. Obsługa NAT46, NAT64, DNS64
   c. Wsparcie dla STUN
7. Polityka bezpieczeństwa systemu:
   a. Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, 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, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego
   d. Musi być w stanie skonfigurować agregowane polityki

    e. Musi być w stanie ograniczyć sesje na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu aplikacji (mysql, ms-sql, sqlnet, pobieranie P2P)
8. Wydzielenie stref bezpieczeństwa:
    a. Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN
    b. Musi mieć możliwość konfiguracji oddzielnych wirtualnych routerów
    c. Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników
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, SMB
    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, BZIP2, TAR, a także wykrywać wielowarstwowe pliki skompresowane dla nie mniej niż 5 warstw dekompresji
10. Równoważenie obciążenia:
    a. Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łącza dla określonej nazwy domeny oraz monitorowanie stanu łącza poprzez aktywną metodę wykrywania
    b. Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted leastconnection i weighted round-robin
    c. Kontrola stanu serwera, 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 12000 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
    d. Możliwość budowania własnych niestandardowych reguł IPS
12. Obrona przed atakiem:
    a. Ochrona przed nieprawidłowym działaniem protokołu
    b. Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment itp.
    c. Wsparcie IPv4 jak i IPv6 dla ochrony przed DNS query flood i DNS reply flood
    d. Biała lista docelowych 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 4700 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. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków.
    b. Możliwość zdefiniowania własnej bazy kategorii www.
    c. Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL.
    d. Kategoria takie jak hazard, malware, spam, botnety
    e. Obsługa Safe Search

f. Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne
g. Dostosowanie strony ostrzeżenia

16. Ochrona danych:
    a. Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy
    b. Identyfikacja protokołu pliku, w tym HTTP,FTP、SMTP, POP3、IMAP
    c. Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS
    d. Filtrowanie plików przesyłanych przez SMB
17. 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
18. 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
    c. Wsparcie wykrywania tunelowania DNS
    d. Wyrywanie i blokowanie DGA
19. 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 i SMB
    c. Obsługa typów plików : PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów
    d. Obsługa blokowania wyników wykrywania w celu szybkiego blokowania nieznanych zagrożeń
20. 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
        iv. Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA
    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. Obsługa dwuskładnikowego uwierzytelniania, SMSy, certyfikaty i tokeny
21. Raportowanie i przeglądanie logów:
    a. Wbudowany w system bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie
    b. W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż:
        i. Posiadanie predefiniowanych raportów dla ruchu internetowego, modułu IPS, skanera antywirusowego i antyspamowego
        ii. Generowanie co najmniej 10 rodzajów raportów
22. 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. Full mesh HA
        iii. Geograficznie rozproszony HA
23. 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.

24. 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
25. 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 bez instalowania oddzielnego oprogramowania, takiego jak dedykowana konsola
26. Gwarancja – Dostawa musi zawierać również:
    a. 24-miesięczną gwarancję producenta na dostarczone elementy systemu
    b. Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 24 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

III. Dostawa urządzenia wraz z oprogramowaniem (2 szt.)- GOPS.

Minimalne parametry techniczne i funkcjonalne:

1. Elementy systemu bezpieczeństwa:
    a. Urządzenie musi mieć możliwość jednoczesnej pracy w trybie Layer 3 (routing), transparentnym (most) i Layer 2 (port mirroring) bez konieczności wirtualizacji sprzętu
    b. Możliwość stworzenia minimum 64 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q.
    c. W zakresie Firewall, obsługa nie mniej niż 450 000 jednoczesnych połączeń i 48 000 nowych połączeń na sekundę.
    d. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o minimalnej pojemności 8 GB do celów logowania i raportowania.
    e. Musi istnieć możliwość rozbudowy o dodatkowy dysk SSD, nie mniejszy niż 256GB
    f. Musi posiadać 2x USB 3.0
    g. Musi posiadać 1x port konsoli
    h. Musi posiadać 1 dedykowany port do zarządzania, minimum Gigabit Ethernet
    i. System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu.
    j. System pełniący funkcję zapory musi posiadać nie mniej niż: 8 interfejsów sieciowych GE
    k. System musi posiadać możliwość wykorzystania portu USB jako Modemu WAN 4G
    l. System musi posiadać zewnętrzy przycisk, pozwalając na reset urządzenia do ustawień fabrycznych, bez konieczności logowania się do urządzenia
    m. Urządzenie musi zostać dostarczone w formie desktopowej
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.) oraz ograniczanie nowych połączeń i jednoczesnych sesji
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 5 Gb/s
    c. Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym IPS i kontrolą aplikacji 1.7 Gb/s
    d. Wydajność ochrony przed atakami (IPS) minimum 2.8 Gb/s
    e. Wydajność AV nie mniej niż 1.8 Gb/s
    f. Wydajność skanowania z włączoną kontrolą aplikacji, AV, IPS, filtrem URL nie mniejsza niż 800 Mb/s.
4. Funkcjonalności VPN:
    a. Wydajność IPSec VPN, nie mniej niż 2.7 Gb/s
    b. Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja
    c. Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem.
    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: 1,2,5,19,20,21,24
    h. Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,19,20,21,24
    i. Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance) co najmniej w zakresie:
        i. Wersji systemu operacyjnego
        ii. Zaaplikowanych patchy
        iii. Ustawień internetowych
        iv. Zainstalowanego oprogramowania antywirusowego
        v. Włączonego Firewalla
        vi. Walidacji kluczy rejestru
        vii. Walidacji istnienia plików
        viii. Walidacji uruchomionych procesów
        ix. Walidacji uruchomionych lub zainstalowanych serwisów
    j. Możliwość rozszerzania ilości użytkowników VPN odpowiednią licencją
    k. Obsługa PnPVPN (Plug and Play VPN)
5. Routing:
    a. Rozwiązanie musi zapewniać: obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP, IS-IS
    b. Obsługa Policy Based Routing
    c. Funkcjonalność Virtual Wire
6. Translacja adresów NAT:
    a. Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego.
    b. Obsługa NAT46, NAT64, DNS64
    c. Wsparcie dla STUN
7. Polityka bezpieczeństwa systemu:

a. Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje bezpieczeństwa, rejestrowanie zdarzeń i zarządzanie pasmem sieci (w tym gwarantowaną i maksymalną przepustowość, priorytety).
b. Możliwość budowania min. 4000 polityk
c. Musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego
d. Musi być w stanie skonfigurować agregowane polityki
e. Musi być w stanie ograniczyć sesje na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu aplikacji (mysql, ms-sql, sqlnet, pobieranie P2P)

8. Wydzielenie stref bezpieczeństwa:
    a. Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN
    b. Musi mieć możliwość konfiguracji oddzielnych wirtualnych routerów
    c. Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników
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, SMB
    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, BZIP2, TAR, a także wykrywać wielowarstwowe pliki skompresowane dla nie mniej niż 5 warstw dekompresji
10. Równoważenie obciążenia:
    a. Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łącza dla określonej nazwy domeny oraz monitorowanie stanu łącza poprzez aktywną metodę wykrywania
    b. Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted leastconnection i weighted round-robin
    c. Kontrola stanu serwera, 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
    d. Możliwość budowania własnych niestandardowych reguł IPS
12. Obrona przed atakiem:
    a. Ochrona przed nieprawidłowym działaniem protokołu
    b. Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment itp.
    c. Wsparcie IPv4 jak i IPv6 dla ochrony przed DNS query flood i DNS reply flood
    d. Biała lista docelowych 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 4700 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. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków.
b. Możliwość zdefiniowania własnej bazy kategorii www.
c. Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL.
d. Kategoria takie jak hazard, malware, spam, botnety
e. Obsługa Safe Search
f. Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne
g. Dostosowanie strony ostrzeżenia

16. Ochrona danych:
    a. Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy
    b. Identyfikacja protokołu pliku, w tym HTTP,FTP、SMTP, POP3、IMAP
    c. Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS
    d. Filtrowanie plików przesyłanych przez SMB
17. 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
18. 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
    c. Wsparcie wykrywania tunelowania DNS
    d. Wyrywanie i blokowanie DGA
19. 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 i SMB
    c. Obsługa typów plików : PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów
    d. Obsługa blokowania wyników wykrywania w celu szybkiego blokowania nieznanych zagrożeń
20. 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
        iv. Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA
    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. Obsługa dwuskładnikowego uwierzytelniania, SMSy, certyfikaty i tokeny
    f. System musi posiadać moduł ZTNA, w celu uwierzytelniania użytkowników bazując na regułach i zasadach zdefiniowanych przed administratora
21. Raportowanie i przeglądanie logów:
    a. Wbudowany w system bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie
    b. W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż:

i. Posiadanie predefiniowanych raportów dla ruchu internetowego, modułu IPS, skanera antywirusowego

ii. Generowanie co najmniej 10 rodzajów raportów

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, Telnet) bez instalowania oddzielnego oprogramowania, takiego jak dedykowana aplikacja
25. Gwarancja – Dostawa musi zawierać również:
    a. 24-miesięczną gwarancję producenta na dostarczone elementy systemu
    b. Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 24 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

.