OPIS PRZEDMIOTU ZAMÓWIENIA

I. Dostarczenie sprzętu wraz wymaganymi licencjami na okres 36 miesięcy od wdrożenia:

a. 2 szt. Firewall działający w klastrze active-passive (urządzenie centralne, siedziba główna),

b. 2 szt. Firewall urządzenia na lokalizacjach wyniesionych (2 lokalizacje),

c. 1 szt. urządzenia dostępowe dla urządzeń serwisowych (hala serwisowa w lokalizacji przy siedzibie głównej).

II. Usługi:

a. szkolenie administratorskie dla dwóch administratorów (dopuszczalne w formie zdalnej),

b. wsparcie w przygotowaniu do wdrożenia produkcyjnego zapory sieciowej(przygotowanie dokumentacji przedwdrożeniowej i powdrożeniowej), przeglądzie obecnej konfiguracji Zmawiającego (dopuszczalne w formie zdalnej),

c. instalacja nowych urządzeń, konfiguracja wstępna, fizyczne uruchomienie i testy (prace stacjonarne),

d. poprawki i rekonfiguracje (dopuszczalne w formie zdalnej),

e. asysta wdrożenia produkcyjnego (dopuszczalne w formie zdalnej),

f. dostarczenie dokumentacji powdrożeniowej pozwalającej na otworzenie konfiguracji i ponowną instalację.

g. Udzielenie gwarancja: dostarczony sprzęt i oprogramowanie musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

III. Obecne rozwiązanie wykonawcy pocztowe:

Zamawiający korzysta z produktów Office 365 oraz posiada poczty w ramach usług Microsoft Exchange oraz Google Gmail.

Licencje:

i. Stosowane licencje w organizacji to Exchange Online (Plan 1) oraz Microsoft 365 Business Standard.

ii. W ramach rozwiązania obecnie Zamawiający posiada:
- active users (133 szt. – w tym z przypisanymi licencjami 94 szt.),
- active teams&grups (35 szt.),
- shared mailboxes (34 szt.),
- distribution list (5 szt.).

iii. Dodatkowo korzysta również z Google Workspace Business Starter (4 szt.)

IV. Firewall obecne stosowane przez Zamawiającego

Sztuk	Nazwa	Licencje	Lokalizacja
2	SOPHOS XG210	XG 210 Enhanced to Enhanced Plus Support (SKU: EP212CEUP), XG 210 Email Protection (SKU: XM212CTAA), XG 210 Webserver Protection (SKU: XS212CTAA), XG 210 Xstream Protection - (SKU: XX212CTES)	Siedziba Główna
2	SOPHOS XG86	XG 86 Xstream Protection (SKU: XX8B2CTES), XG 86 Webserver Protection - (SKU: XS8B2CTAA), XG 86 Email Protection - (SKU: XM8B2CTAA)	Lokalizacja 1, Lokalizacja 2
1	Zyxel USG60W	LIC-BUN for USG60 & USG60W, Filtering/Anti-Virus Bitdefender Signature/SecuReporter Premium License, LIC-BUN for USG60 & USG60W, Content Filtering/Anti-Virus Bitdefender Signature/SecuReporter Premium License	Hala serwisowa (Siedziba Główna)

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym oraz przeszkolić z ich obsługi.

Załącznik nr 4 do zapytania ofertowego – Opis przedmiotu zamówienia

1. System ochrony poczty – wymagania minimalne

a. Zgodność z wszystkimi dostawcami usług e-mail

Musi być kompatybilny ze wszystkimi usługami e-mail, w tym Google Workspaces Gmail i Microsoft 365:

- Microsoft Exchange Online i Microsoft 365
- Microsoft Exchange 2003 lub nowszy
- Google Workspaces Gmail

b. Integracja z Microsoft 365 Mailflow Rules

- Musi być w stanie stworzyć bezpośrednie połączenie z Microsoft 365 z poziomu konsoli administracyjnej, bez potrzeby przekierowań rekordów MX.
- Musi mieć możliwość korzystania z API Microsoft do tworzenia reguł przepływu poczty w środowisku Microsoft 365.

c. Ochrona przed manipulacją regułami przepływu poczty

- Musi ostrzegać klientów o wszelkich zmianach konfiguracji w konsoli M365, które mogą wpływać na konfigurację bramy poczty e-mail, przywracanie i korektę konfiguracji i przepływu poczty.

d. Zarządzanie w chmurze

- Musi chronić i zarządzać e-mailami w chmurze za pomocą intuicyjnej konsoli opartej na technologii chmurowej, zapewniając dostęp do pełnego zakresu produktów dostawcy przez jeden interfejs/konsole, w tym: web, endpoint, mobile i server.
- Musi mieć możliwość tworzenia unikalnych polityk bezpieczeństwa e-mail dla osób, grup lub całej domeny.
- Musi mieć opcję klonowania istniejącej polityki w konsoli administracyjnej.
- Musi zapewniać dostęp administracyjny do listy dozwolonych i blokowanych adresów użytkowników końcowych z możliwością importowania, eksportowania, wyszukiwania, dodawania i usuwania wpisów bezpośrednio z poziomu konsoli administracyjnej.
- Musi być w stanie dodawać tekstowe i HTML-owe klauzule wyjściowe do wiadomości, które można skonfigurować przez politykę bezpieczeństwa e-mail w konsoli administracyjnej.

e. Synchronizacja z Active Directory, Azure Active Directory i Google Directory

- Musi mieć możliwość synchronizacji z Microsoft Active Directory.
- Musi mieć możliwość synchronizacji z Microsoft Azure Active Directory.
- Musi być w stanie automatycznie synchronizować użytkowników z produktem przy użyciu narzędzia do synchronizacji Active Directory.
- Musi w pełni wspierać automatyczne aktualizowanie danych AD~~,~~
- Musi wspierać synchronizację z Google Directory.
- Musi zapewniać administratorowi możliwość ręcznego dodawania skrzynek pocztowych lub importowania skrzynek pocztowych i aliasów, gdy Active Directory jest niedostępny.

f. Portal samoobsługowy dla użytkowników końcowych

- Musi mieć portal samoobsługowy dla użytkowników końcowych.
- Portal samoobsługowy musi umożliwiać użytkownikom zarządzanie kwarantanną e-mail (akceptowanie/usuwanie wiadomości).
- Portal samoobsługowy musi umożliwiać użytkownikom edytowanie reguł dozwolonych/blokowanych.
- Portal samoobsługowy musi umożliwiać użytkownikom przeglądanie wiadomości w przypadku awarii przy użyciu awaryjnej skrzynki odbiorczej.
- Portal dla użytkowników końcowych musi pozwalać na zwalnianie wiadomości na żądanie, a w dziennikach kwarantanny musi być możliwość codziennego podsumowania wiadomości w kwarantannie, z opcją zwolnienia bezpośrednio ze skrzynki odbiorczej.

g. Ciągłość biznesowa

- Musi mieć możliwość przechowywania e-maili w buforze, co zapewnia, że żadna wiadomość nie zostanie utracona.
- W przypadku zakłóceń w usłudze e-mail Microsoft lub Google Cloud, produkt musi mieć możliwość automatycznego kolejkowania wiadomości odbiorcy, a następnie dostarczenia ich po przywróceniu usługi z minimum pięciodniowym okresem ponownych prób.
- Musi zapewniać dostęp do kolejkowanych wiadomości e-mail z poziomu 24/7 awaryjnej skrzynki odbiorczej wewnątrz portalu użytkownika końcowego.
- Musi mieć możliwość wysyłania alertów administratora, gdy poczta nie może być dostarczona do serwera/usługi w przypadku awarii usługi poczty e-mail dostarczanej przez zewnętrznego dostawcę.

h. Ochrona przed spamem i złośliwym oprogramowaniem

- Musi mieć aktualizacje zagrożeń w czasie rzeczywistym, aby zatrzymać najnowsze ataki.
- Musi wykrywać spam, wirusy i phishing.
- Musi mieć filtrowanie reputacji, które może blokować spam.
- Musi mieć technologię filtrowania reputacji nowej generacji, która eliminuje spam botnetowy na poziomie połączenia IP, monitorując żądania połączeń i odrzucając te, które wykazują oznaki połączeń botnetowych.
- Musi chronić przed spamem typu snowshoe.

i. Aktywna ochrona przed zagrożeniami

- Musi mieć możliwość przepisania URL do sprawdzenia reputacji witryny linków e-mail przed dostarczeniem i w momencie kliknięcia - blokowanie podstępnych, opóźnionych ataków.
- Musi mieć chmurowy sandbox, który może wykrywać zarówno znane, jak i nieznane złośliwe oprogramowanie oraz niechciane aplikacje przed ich uruchomieniem.
- Musi mieć opcję przesyłania e-maili w kwarantannie do skanowania w chmurowym sandboxie z poziomu konsoli administracyjnej.

j. Ochrona po dostarczeniu

- Musi mieć możliwość automatycznego usuwania wiadomości zawierających załączniki i URL-e, które są bezpieczne w momencie dostarczenia, ale później stają się aktywne i złośliwe.

- Musi mieć funkcję wycofywania na żądanie, która pozwala administratorom ręcznie usuwać dowolną wiadomość ze skrzynek odbiorczych użytkowników za pomocą jednego kliknięcia w konsoli administracyjnej.

k. Blokowanie phishingu

- Musi używać kombinacji technik uwierzytelniania w celu identyfikacji i dopuszczania legalnych wiadomości e-mail od zaufanych partnerów oraz blokowania oszustów.
- Musi używać sprawdzania Sender Policy Framework (SPF), aby zidentyfikować adresy IP upoważnione do wysyłania e-maili z domeny.
- Musi używać Domain Keys Identified Mail (DKIM), aby zapewnić kryptograficzny dowód, że wiadomość została wysłana od określonego nadawcy i nie została zmieniona.
- Musi używać sprawdzania Domain Message Authentication Reporting & Conformance (DMARC), aby określić, co zrobić, gdy wiadomości nadawcy nie przejdą sprawdzeń SPF lub DKIM.
- Musi mieć wykrywanie anomalii nagłówków, aby zidentyfikować, czy nazwa wyświetlana nadawcy jest taka sama jak jedna z nazw użytkowników wewnętrznych.
- Musi być w stanie porównywać nazwy wyświetlane przychodzących e-maili z nazwami wyświetlanymi powszechnie używanych usług chmurowych oraz VIP-ów w organizacji, aby sprawdzić, czy występują dopasowania.
- Musi być w stanie przeprowadzić analizę podobnych domen, aby zidentyfikować nazwy domen podobne do domeny Zamawiającego.
- Podejrzane wiadomości powinny mieć opcję blokowania, kwarantanny, oznaczania ostrzeżeniem w temacie lub dodawania banera z bezpośrednim linkiem do listy zablokowanych na poziomie użytkownika.
- Musi mieć politykę dozwolonych i zablokowanych nadawców, która pozwala administratorom na ograniczanie wiadomości do lub z określonych adresów e-mail, adresów IP i domen, w tym obsługę znaków wieloznacznych, umożliwiającą blokowanie TLD na poziomie kraju.
- Smart Banners muszą pozwalać użytkownikom na aktualizację ich spersonalizowanych list dozwolonych i zablokowanych nadawców bezpośrednio z poziomu e-maila, podczas gdy portal samoobsługowy pozwala na zarządzanie tymi listami.

l. Zapobieganie utracie danych

- Musi automatycznie skanować treści wiadomości i załączniki pod kątem wrażliwych danych, aby łatwo ustalać polityki blokowania lub szyfrowania wiadomości.
- Musi dawać użytkownikom możliwość szyfrowania e-maili przy użyciu dodatku M365 produktu.
- Musi mieć szyfrowanie end-to-end encryption (E2EE), które chroni całą wiadomość lub tylko załączniki.
- Musi mieć wymuszone szyfrowanie TLS, które zapobiega podsłuchiwaniu wiadomości w tranzycie.
- Musi mieć możliwość dodawania cyfrowego podpisu do weryfikacji tożsamości nadawcy za pomocą S/MIME.
- Musi mieć opcjonalne pełne szyfrowanie portalu internetowego które pozwala użytkownikom zarządzać, czytać i odpowiadać na zaszyfrowane wiadomości w bezpiecznym portalu internetowym.

- Musi być w stanie tworzyć wielozadaniowe polityki kontroli danych dla grup i indywidualnych użytkowników, aby zapewnić ochronę wrażliwych informacji z wykrywaniem danych finansowych, treści poufnych, informacji zdrowotnych i PII we wszystkich e-mailach i załącznikach.
- Musi być w stanie tworzyć niestandardowe listy kontrolne treści (CCL) przy użyciu list CCL dostawcy lub dostosowywać szablony z pudełka do specyficznych CCL.
- Musi mieć granularną kontrolę polityk zapobiegania wyciekom danych, w tym polityk wielozadaniowych dla grup i indywidualnych użytkowników z bezproblemową integracją szyfrowania.
- Musi być w stanie sprawdzać atrybuty dowolnego e-maila, korzystając z reguły atrybutów wiadomości w polityce kontroli danych.
- Polityka kontroli danych musi mieć opcję atrybutów wiadomości, która pozwala administratorom na filtrowanie wiadomości według nagłówka, źródła i rozmiaru.
- Polityka kontroli danych musi mieć akcję modyfikowania nagłówka z następującymi opcjami:
  - dodaj nagłówek – wstawia nowy nagłówek i wartość do wiadomości
  - edytuj wartość nagłówka – edytuje wartości wszystkich dopasowanych nagłówków
  - usuń nagłówek – usuwa wszystkie dopasowane nagłówki
- Konsola administracyjna musi umożliwiać administratorom usuwanie, ponowne załączanie lub pobieranie załączników z wiadomości w kwarantannie.

m. Kompleksowe raportowanie i autoryzacja

- Musi generować statystyki raportów w konsoli w formie tabel i wykresów z niestandardowymi zakresami dat.
- Musi generować następujące raporty:
  - Historia wiadomości (pokazuje dzienniki wszystkich przetworzonych przez system wiadomości)
  - Podsumowanie wiadomości (pokazuje podsumowanie wszystkich wiadomości)
  - Podsumowanie zaawansowanych zagrożeń sandbox (raporty werdyktów, w tym wyniki VirusTotal i taktyki MITRE ATT&CK Matrix)
  - Podsumowanie czasu kliknięcia (ilość zablokowanych, ostrzeżonych i dozwolonych URL-i)
  - Naruszenia DLP (wiadomości zalogowane przez polityki DLP)
  - Podsumowanie po dostarczeniu (podsumowanie wiadomości M365 usuniętych po dostarczeniu)
  - Podsumowanie użycia licencji
- Musi mieć API, które umożliwia zapytania o historię wiadomości z jeziora danych (ang. Data lake) dostawcy przy użyciu konsoli administracyjnej.
- Dostarczone rozwiązanie musi obsługiwać raportowanie w formacie Syslog w celu przekazywania danych do zewnętrznego serwera logów.

Logowanie administratorów za pomocą dwu-składnikowego uwierzytelniania z wykorzystaniem tokenów sprzętowych lub oprogramowania. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub wskazane oprogramowanie (darmowe lub płatne w przypadku płatnych dostarczenie co najmniej 4 licencji), które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. (Zamawiający posiada klucze YubiKey 5 NFC (jeżeli można je zastosować dostawa nie dotyczy) oraz korzysta z Microsoft Authenticator)**n. Dostarczone rozwiązanie musi pozwalać na rozbudowę w przyszłości p**

połączenie z innymi produktami bezpieczeństwa od dostawcy Firewall (nie dostarczane w dniu zamówienia):

- Musi mieć możliwość połączenia rozwiązań bezpieczeństwa e-mail i ochrony punktów końcowych dostawcy, aby automatycznie izolować skompromitowane skrzynki pocztowe i czyścić zainfekowane komputery wysyłające wychodzący spam i złośliwe oprogramowanie.
- Musi mieć możliwość połączenia rozwiązań bezpieczeństwa e-mail i szkoleń z zakresu bezpieczeństwa dostawcy, aby umożliwić zapisywanie ryzykownych użytkowników na ukierunkowane szkolenia edukacyjne z jednym kliknięciem.

2. Firewall – 2 sztuki – wymagania minimalne

	System	
2.1	**Konstrukcja**	
2.1.1	System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania.	
2.1.2	Rozwiązanie musi być wyposażone w moduł kryptograficzny zgodny ze standardem FIPS 140-2.	
2.1.3	Rozwiązanie musi wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca)	
2.1.4	Rozwiązanie musi ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie Active-Passive lub Active-Active.	
2.1.5	System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej.	
2.1.6	Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy (drugi zasilacz jako wyposażenie opcjonalne).	
2.1.7	Urządzenie w metalowej obudowie z możliwością montażu w szafie rack 19".	
2.1.8	Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB).	
2.1.9	Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie.	
2.1.10	Możliwość przeprowadzenia konfiguracji w trybie Zero Touch.	
2.1.11	Pamięć operacyjna RAM nie mniej niż (GB):	8
2.1.12	Przestrzeń do przechowywania logów i raportów nie mniej niż (GB)	120
2.1.13	Liczba fizycznych interfejsów 1000BASE-T nie mniej niż:	8
2.1.14	Liczba fizycznych interfejsów 1000BASE-X nie mniej niż:	2
2.1.15	Liczba fizycznych interfejsów 10GBASE-X nie mniej niż:	4
2.1.16	Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q nie mniej niż:	256
2.2	**Wydajność**	
2.2.1	Wydajność Firewall nie mniej niż (Mbps)	35000
2.2.2	Wydajność Firewall IMIX nie mniej niż (Mbps)	18000
2.2.3	Wydajność IPS nie mniej niż (Mbps)	65000
2.2.4	Wydajność FW+IPS+AV nie mniej niż (Mbps)	1500
2.2.5	Wydajność NGFW nie mniej niż (Mbps)	6000
2.2.6	Liczba równoczesnych połączeń nie mniejsza niż:	6000000
2.2.7	Liczba nowych połączeń na sekundę nie mniejsza niż:	140000
2.2.8	Wydajność IPsec VPN nie mniej niż (Mbps):	20000
2.2.9	Wydajność dla inspekcji ruchu SSL/TLS nie mniej niż (Mbps):	1250
2.2.10	Liczba równoczesnych połączeń SSL/TLS nie mniejsza niż:	15000
2.2.11	Liczba równoczesnych tuneli SSL VPN nie mniejsza niż:	1000

2.2.12	Liczba równoczesnych tuneli IPsec VPN nie mniejsza niż:	1000
2.3	**Zarządzanie**	
2.3.1	Rozwiązanie musi być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym.	
2.3.2	Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA).	
2.3.3	Rozwiązanie musi oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN.	
2.3.4	Wbudowany webowy graficzny interfejs administratora musi oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter.	
2.3.5	Interfejs graficzny administratora musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.	
2.3.6	Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.	
2.3.7	System musi oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności.	
2.3.8	System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.	
2.3.9	System musi oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.	
2.3.10	Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).	
2.3.11	System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów musi być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.	
2.3.12	Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm).	
2.3.13	System musi oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog).	
2.3.14	Rozwiązanie musi zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej.	
2.3.15	System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS).	
2.3.16	Rozwiązanie musi oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta.	
2.3.17	System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpowiednik).	
2.3.18	System musi zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia.	

2.3.19	System musi oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta
2.3.20	Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji.
2.3.21	Dostarczony system musi posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.
	Zapora sieciowa, konfiguracja sieciowa oraz routing
2.4	**Zapora sieciowa**
2.4.1	Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection.
2.4.2	System musi umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6.
2.4.3	Rozwiązanie musi umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas.
2.4.4	Rozwiązanie musi zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.
2.4.5	Rozwiązanie musi oferować możliwość definiowania własnych stref zapory sieciowej.
2.4.6	System musi umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).
2.4.7	System musi pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika.
2.5	**Trasowanie ruchu**
2.5.1	Rozwiązanie musi oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing.
2.5.2	Rozwiązanie musi zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.
2.5.3	Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów.
2.5.4	Rozwiązanie musimusi zapewniać obsługę routingu statycznego dla ruchu unicast i multicast.
2.5.5	Rozwiązanie musimusi zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).
2.5.6	Rozwiązanie musimusi zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM).
2.5.7	Rozwiązanie musimusi zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6.
2.6	**Translacja adresów i portów**
2.6.1	Rozwiązanie musi pozwolić na definiowanie niezależnych od reguł zapory polis NAT.
2.6.2	Rozwiązanie musi pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT
2.7	**Kształtowanie pasma i jakość usług**
2.7.1	System musi zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji.
2.7.2	Rozwiązanie musi pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.
2.7.3	System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
2.7.4	Podczas klasyfikacji usług rozwiązanie musi uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6.

2.7.5	Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet.
2.8	**Podstawowa ochrona przed atakami DoS i DDoS**
2.8.1	System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
2.9	**Pozostałe**
2.9.1	Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.
2.9.2	Rozwiązanie musi oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge).
2.9.3	System musi oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.
2.9.4	System musi oferować wsparcie dla IEEE 802.3Q VLAN z możliwością konfiguracji niezależnych puli DHCP.
2.9.5	Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).
2.9.6	System musi oferować wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp.
2.9.7	Rozwiązanie musi zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).
2.9.8	Rozwiązanie musi obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo).
2.9.9	Rozwiązanie musi umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych.
2.10	**Uwierzytelnianie i obsługa użytkowników**
2.10.1	Wymagane uwierzytelnianie użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta.
2.10.2	Rozwiązanie musi być wyposażone w lokalną bazę użytkowników.
2.10.3	System musi zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+.
2.10.4	Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory.
2.10.5	System musi umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm).
2.10.6	Rozwiązanie musi umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server.
2.10.7	System musi oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.
2.10.8	Rozwiązanie musi oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci.
2.10.9	Rozwiązanie musi umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania.
2.10.10	Rozwiązanie musi umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS.
2.10.11	Rozwiązanie musi umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android.
2.10.12	Rozwiązanie musi umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu.
2.11	**Koncentrator VPN**
2.11.1	System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2.

2.11.2	System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519).
2.11.3	System musi obsługiwac połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN.
2.11.4	Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN.
2.11.5	Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback.
2.11.6	Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego.
2.11.7	Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth.
2.11.8	Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połaczeń IPsec client-to-site VPN jak i SSL client-to-site VPN.
2.11.9	Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN.
2.11.10	Urządzenie musi obsługiwać połączenia L2TP over IPsec.
2.12	**Logowanie i raportowanie**
2.12.1	System musi możliwiać monitorowanie logów ruchu w czasie rzeczywistym.
2.12.2	System musi umożliwiać składowanie oraz archiwizację logów.
2.12.3	Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
2.12.4	Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów.
2.12.5	Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa
2.12.6	System musi zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali.
2.12.7	System musi zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących.
2.12.8	Rozwiązanie musi umożliwiać wysyłanie raportów via email.
2.12.9	Rozwiązanie musi umożliwiać eksport raportów do plików PDF, HTML i CSV.
2.12.10	Rozwiązanie musi oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.
2.12.11	System musi zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.
2.12.12	System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację.
2.12.13	Rozwiązanie musi oferować możliwość zanonimizowania danych w raportach.
2.12.14	System musi umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.
2.13	**Intrusion Prevention System i Advanced Threat Protection**
2.13.1	Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur.
2.13.2	Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.
2.13.3	Rozwiązanie musi umożliwiać tworzenie własnych sygnatur IPS.
2.13.4	Rozwiązanie musi umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS.
2.13.5	System ochrony musi zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet.
	Ochrona i kontrola web

2.14	**Ochrona przez Malware**
2.14.1	Rozwiązanie musi działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP.
2.14.2	Rozwiązanie musi wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania.
2.14.3	Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.
2.14.4	System musi filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.
2.14.5	Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek.
2.14.6	Rozwiązanie musi przeprowadzać emulację skryptów Java.
2.14.7	Rozwiązanie musi przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta.
2.14.8	System musi umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates)
2.15	**Inspecja ruchu SSL/TLS**
2.15.1	Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów.
2.15.2	Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2.
2.15.3	Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP.
2.15.4	Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443).
2.15.5	Rozwiązanie musi umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web.
2.15.6	Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen.
2.16	**Filtr Web**
2.16.1	Filtrowanie stron web musi być oparte o predefiniowane kategorie z możliwością tworzenia własnych kategorii stron.
2.16.2	Rozwiązanie musi umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy.
2.16.3	Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól.
2.16.4	System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator musi mieć możliwość modyfikowamoa treści komunikatu w tym dodania logo organizacji.
2.17	**Ochrona i kontrola aplikacji**
2.17.1	Rozwiązanie musi oferować bazę danych opisująca co najmniej 3000 aplikacji.
2.17.2	Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji.
2.17.3	Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikro-aplikacji.
2.17.4	Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów.
2.17.5	Rozwiązanie musi umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp.
2.17.6	Rozwiązanie musi umożliwiać tworzenie własnych grup aplikacji co najmniej na potrzeby polityk SD-WAN.
2.18	**Ochrona przed nieznanymi zagrożeniami**
2.18.1	Rozwiązanie klasy Sandbox do ochrony przez zagrożeniami typu Zero-Day.

2.18.2	Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll.
2.18.3	Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf.
2.18.4	Rozwiązanie umożliwiające dodatkową inspekcję i deponację plików .pdf.
2.18.5	Rozwiązanie umożliwiające dodatkową inspekcję i deponację archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab.
2.18.6	Rozwiązanie nie może mieć ograniczeń co do liczby analizowanych plików.
2.18.7	System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS.
2.18.8	System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu.
2.18.9	System zapewniający ochronę przed exploitami i złośliwym kodem ransomware.

3. Firewall – 2 sztuki – wymagania minimalne

	System	
3.1	**Konstrukcja**	
3.1.1	System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania.	
3.1.2	Rozwiązanie musi być wyposażone w moduł kryptograficzny zgodny ze standardem FIPS 140-2.	
3.1.3	Rozwiązanie musi wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca)	
3.1.4	Rozwiązanie musi ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie HA Active-Passive lub Active-Active.	
3.1.5	System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej.	
3.1.6	Rozwiązanie musi być wyposażone w wysokowydajny wielordzeniowy procesor x86 (CPU) oraz dodatkowo w procesor (NPU) do akceleracji ruchu dla warstwy aplikacji.	
3.1.7	Urządzenie w metalowej obudowie o wysokości 1U z możliwością montażu w szafie rack 19" (uchwyty montażowe jako opcjonalne wyposażenie).	
3.1.8	Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB).	
3.1.9	Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie.	
3.1.10	Wbudowany port USB umożliwiający podłączenie pamięci flash i przeprowadzenie konfiguracji w trybie Zero Touch.	
3.1.11	Pamięć operacyjna RAM nie mniej niż (GB):	4
3.1.12	Przestrzeń do przechowywania logów i raportów nie mniej niż (GB)	16
3.1.13	Liczba fizycznych interfejsów 1000BASE-T nie mniej niż:	4
3.1.14	Liczba fizycznych interfejsów 1000BASE-X nie mniej niż:	1
3.1.15	Liczba fizycznych interfejsów 10GBASE-X nie mniej niż:	-
3.1.16	Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q nie mniej niż:	128
3.2	**Wydajność**	
3.2.1	Wydajność Firewall nie mniej niż (Gbps)	3,85
3.2.2	Wydajność Firewall IMIX nie mniej niż (Gbps)	3
3.2.3	Wydajność IPS nie mniej niż (Gbps)	1,2
3.2.4	Wydajność FW+IPS+AV nie mniej niż (Gbps)	0,28
3.2.5	Wydajność NGFW nie mniej niż (Gbps)	0,7
3.2.6	Liczba równoczesnych połączeń nie mniejsza niż:	1600000
3.2.7	Liczba nowych połączeń na sekundę nie mniejsza niż:	35700

3.2.8	Wydajność IPsec VPN nie mniej niż (Gbps):	3
3.2.9	Wydajność dla inspekcji ruchu SSL/TLS nie mniej niż (Gbps):	0,375
3.2.10	Liczba równoczesnych połączeń SSL/TLS nie mniejsza niż:	8192
3.2.11	Liczba równoczesnych tuneli SSL VPN nie mniejsza niż:	500
3.2.12	Liczba równoczesnych tuneli IPsec VPN nie mniejsza niż:	500
3.3	**Zarządzanie**	
3.3.1	Rozwiązanie musi być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym.	
3.3.2	Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA).	
3.3.3	Rozwiązanie musi oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN.	
3.3.4	Wbudowany webowy graficzny interfejs administratora musi oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter.	
3.3.5	Interfejs graficzny administratora musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.	
3.3.6	Rozwiązanie musi oferować wiersz poleceń dostępny z poziomu graficznego interfejsu administraotra, portu konsolowego oraz za pośrednictwem protokołu SSH z uwierzytelnianiem przy użyciu kluczy RSA, DSA lub ECDSA o długości min. 2048 bitów.	
3.3.7	Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.	
3.3.8	System musi oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności.	
3.3.9	System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.	
3.3.10	System musi oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.	
3.3.11	Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).	
3.3.12	System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów musi być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.	
3.3.13	Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm).	
3.3.14	System musi oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog).	
3.3.15	Rozwiązanie musi zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej.	
3.3.16	System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS).	
3.3.17	Rozwiązanie musi oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta.	
3.3.18	System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpowiednik).	

3.3.19	System musi zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia.
3.3.20	System musi oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta, przy czym w podstawowej wersji utrzymywany i udostępniany jest on bezpłatnie i nie wymaga zakupu osobnych subskrypcji.
3.3.21	Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP, via email jak i dodatkowo do centralnego systemu zarządzania w chmurze.
3.3.22	Rozwiązanie musi oferować wbudowany mechanizm pozwalający na automatyczne tworzenie szyfrowanych hasłem kopii zapasowych konfiguracji w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu.
3.3.23	Dostarczony system musi posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.
3.3.24	Rozwiązanie musi zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej.
3.3.25	Zarządzanie licencjami i subskrypcjami musi odbywać się za pośrednictwem portalu licencyjnego a synchronizacja subskrypcji powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami.
3.3.26	Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). Informacja o dostępności nowej wersji powinna pojawiać się w Web GUI.
3.3.27	Producent musi oferować mechanizm automatycznego łatania wykrytych w oprogramowaniu systemowym podatności przez tzw. hotfixies, przy czym administrator musi móc funkcjonalność tą wyłączyć.
3.3.28	Rozwiązanie musi oferować mechanizm szyfrowania danych takich jak loginy, hasła, klucze które przechowywane są w konfiguracji urządzenia. Dane powinny być zabezpieczone dedykowanym kluczem szyfrującym tworzonym na podstawie bezpiecznie składowanego poza urządzeniem hasła.
3.3.29	Rozwiązanie musi zapewniać możliwość zmiany nazw interfejsów sieciowych.
	Zapora sieciowa, konfiguracja sieciowa oraz routing
3.4	**Zapora sieciowa**
3.4.1	Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection.
3.4.2	System musi umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6.
3.4.3	Rozwiązanie musi umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas.
3.4.4	System musi umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.
3.4.5	System musi pozwalać na selektywne wyłączanie reguł zapory sieciowej (bez konieczności ich usuwania).
3.4.6	System musi pozwalać na grupowanie reguł zapory. Wymagana jest funkcjonalność automatycznego wiązania nowotworzonych reguł do właściwych grup na podstawie kryteriów opisujących grupę.
3.4.7	Rozwiązanie musi zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.
3.4.8	System ochrony musi zawierać predefiniowane strefy zapory typu: LAN, WAN, DMZ, VPN.
3.4.9	Rozwiązanie musi oferować możliwość definiowania własnych stref zapory sieciowej.
3.4.10	System musi umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).
3.4.11	Rozwiązanie musi oferować narzędzie do symulowanego testu reguł zapory w oparciu o zadane przez administratora kryteria takie jak IP, strefa zapory, użytkownik, dzień, godzina.
3.4.12	System musi pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika.

3.5	**Trasowanie ruchu**
3.5.1	Rozwiązanie musi oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing.
3.5.2	Rozwiązanie musi zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.
3.5.3	Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów.
3.5.4	Rozwiązanie musi umożliwiać rozkładanie ruchu w oparciu o wagi interfejsów WAN.
3.5.5	Rozwiązanie musi zapewniać obsługę routingu statycznego dla ruchu unicast i multicast.
3.5.6	Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).
3.5.7	Rozwiązanie musi zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM).
3.5.8	Rozwiązanie musi zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6.
3.6	**Translacja adresów i portów**
3.6.1	Rozwiązanie musi pozwolić na definiowanie niezależnych od reguł zapory polis NAT.
3.6.2	Rozwiązanie musi pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT
3.6.3	Rozwiązanie musi pozwalać na automatyczne tworzenie reguł NAT typu loopback czy reflexive rule.
3.7	**Kształtowanie pasma i jakość usług**
3.7.1	System musi zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji.
3.7.2	Rozwiązanie musi pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.
3.7.3	System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
3.7.4	Podczas klasyfikacji usług rozwiązanie musi uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6.
3.7.5	Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet (od 1 Business Critical do 7 Best Effort).
3.8	**Podstawowa ochrona przed atakami DoS i DDoS**
3.8.1	System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
3.9	**Pozostałe**
3.9.1	Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.
3.9.2	Rozwiązanie musi oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge).
3.9.3	System musi oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.
3.9.4	System musi oferować wsparcie dla IEEE 802.1Q VLAN z możliwością konfiguracji niezależnych puli DHCP.
3.9.5	Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).
3.9.6	System musi oferować wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp.
3.9.7	Rozwiązanie musi zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).
3.9.8	Rozwiązanie musi obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo).
3.9.9	Rozwiązanie musi umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych.
3.10	**Kontroler sieci bezprzewodowej**

3.10.1	System musi zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania.
3.10.2	Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Access Point, Wireless Bridge oraz Wireless Repeater.
3.10.3	Uruchomienie punktów dostępowych sieci bezprzewodowej musi odbywać się na zasadzie plug-and-play, gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu.
3.10.4	Zarządzanie punktami dostępowymi sieci bezprzewodowej musi odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej.
3.10.5	Rozgłaszane sieci bezprzewodowe powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując przy tym możliwość izolacji klientów sieci bezprzewodowej.
3.10.6	Rozwiązanie musi umożliwiać rozgłaszanie wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej (Hide SSID).
3.10.7	Rozwiązanie musi oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise.
3.10.8	Rozwiązanie musi zapewniać wsparcie dla uwierzytelniania klientów w oparciu o IEEE 802.1X (RADIUS Authentication).
3.10.9	Rozwiązanie musi oferować wsparcie dla IEEE 802.11r (Fast Transition).
3.10.10	System musi umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów.
3.10.11	Dostęp do sieci bezprzewodowej musi być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości.
3.10.12	System musi zapewniać możliwość tworzenia odseparowanej sieci dla gości w wariancie walled garden.
3.10.13	System musi pozwalać na rozgłaszanie sieci bezprzewodowych w oparciu o harmonogramy czasowe.
3.10.14	Rozwiązanie musi zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych (Rogue AP detection).
3.11	**Uwierzytelnianie i obsługa użytkowników**
3.11.1	Wymagane uwierzytelniaine użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta.
3.11.2	Rozwiązanie musi być wyposażone w lokalną bazę użytkowników.
3.11.3	System musi zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+.
3.11.4	Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory.
3.11.5	System musi umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm).
3.11.6	Rozwiązanie musi umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server.
3.11.7	System musi oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.
3.11.8	Rozwiązanie musi oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci.
3.11.9	Rozwiązanie musi umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania.
3.11.10	Rozwiązanie musi umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS.
3.11.11	Rozwiązanie musi umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android.

3.11.12	Rozwiązanie musi umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu.
3.12	**Koncentrator VPN**
3.12.1	System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2.
3.12.2	System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519).
3.12.3	System musi obsługiwac połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN.
3.12.4	Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN.
3.12.5	Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback.
3.12.6	Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego.
3.12.7	Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth.
3.12.8	Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połaczeń IPsec client-to-site VPN jak i SSL client-to-site VPN.
3.12.9	Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN.
3.12.10	Urządzenie musi obsługiwać połączenia L2TP over IPsec.
3.12.11	Połączenia VPN terminowane muszą być dedykowanej strefie zapory sieciowej.
3.13	**Logowanie i raportowanie**
3.13.1	System musi możliwiać monitorowanie logów ruchu w czasie rzeczywistym.
3.13.2	System musi umożliwiać składowanie oraz archiwizację logów.
3.13.3	Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
3.13.4	Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów.
3.13.5	Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa
3.13.6	System musi zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali.
3.13.7	System musi zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących.
3.13.8	Rozwiązanie musi umożliwiać wysyłanie raportów via email.
3.13.9	Rozwiązanie musi umożliwiać eksport raportów do plików PDF, HTML i CSV.
3.13.10	Rozwiązanie musi oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.
3.13.11	System musi zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.
3.13.12	System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację.
3.13.13	Rozwiązanie musi oferować możliwość zanonimizowania danych w raportach.
3.13.14	System musi umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.
3.14	**Intrusion Prevention System i Advanced Threat Protection**
3.14.1	Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur.
3.14.2	Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.
3.14.3	Rozwiązanie musi umożliwiać tworzenie własnych sygnatur IPS.
3.14.4	Rozwiązanie musi umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS.

3.14.5	System ochrony musi zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet.
	Ochrona i kontrola web
3.15	**Ochrona przez Malware**
3.15.1	Rozwiązanie musi działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP.
3.15.2	Rozwiązanie musi wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania.
3.15.3	Dodatkowo rozwiązanie musi umożliwiać uruchomienie silnika antywirusowego firmy trzeciej.
3.15.4	Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.
3.15.5	System musi filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.
3.15.6	Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek.
3.15.7	Rozwiązanie musi przeprowadzać emulację skryptów Java.
3.15.8	Rozwiązanie musi przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta.
3.15.9	Rozwiązanie musi umożliwiać blokowanie potencjalnie niechcianych aplikacji (tzw. Potentially Unwanted Applications - PUAs)
3.15.10	System musi umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates)
3.16	**Inspecja ruchu SSL/TLS**
3.16.1	Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów.
3.16.2	Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2.
3.16.3	Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP.
3.16.4	Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443).
3.16.5	Rozwiązanie musi umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web.
3.16.6	Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen.
3.17	**Filtr Web**
3.17.1	Rozwiązanie musi zawierać przynajmniej 90 kategorii stron Web oraz umożliwiać dodawanie własnych kategorii stron.
3.17.2	Rozwiązanie musi umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy.
3.17.3	Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól.
3.17.4	System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator musi mieć możliwość modyfikowamoa treści komunikatu w tym dodania logo organizacji.
3.17.5	Rozwiązanie musi umożliwiać filtrowanie stron web analizując ich zawartość wykorzystując tzw. Content Filtering na bazie haseł kluczowych.
3.17.6	Rozwiązanie musi oferować ochronę przed Pharmingiem.
3.18	**Ochrona i kontrola aplikacji**
3.18.1	Rozwiązanie musi oferować bazę danych opisująca co najmniej 3000 aplikacji.
3.18.2	Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji.

3.18.3	Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikro-aplikacji.
3.18.4	Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów.
3.18.5	Rozwiązanie musi umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp.
3.18.6	Rozwiązanie musi oferować funkcje CASB (Cloud Access Security Broker) celem monitorowania i regulowania dostępu do aplikacji chmurowych wykorzystywanych przez użytkowników.
3.18.7	Rozwiązanie musi umożliwiać tworzenie własnych grup aplikacji co najmniej na potrzeby polityk SD-WAN.
3.19	**Ochrona przed nieznanymi zagrożeniami**
3.19.1	Rozwiązanie klasy Sandbox do ochrony przez zagrożeniami typu Zero-Day.
3.19.2	Rozwiązanie oferujące statyczną i dynamiczną analizę kodu przesyłanego w ramach ruchu web czy email.
3.19.3	Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll.
3.19.4	Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf.
3.19.5	Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf.
3.19.6	Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab.
3.19.7	System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS.
3.19.8	System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu.
3.19.9	System zapewniający analizę strukury kodu w tym analizę przeprowadzaną przez mechanizmy głębokiego uczenia maszynowego.
3.19.10	System zapewniający ochronę przed exploitami i złośliwym kodem ransomware.
3.19.11	System badający reputację pliku w zewnętrznych bazach takich jak np.Virustotal.
3.19.12	System musi oferować szczegółowe raporty dowodzące przeprowadzanie analizy dla w/w mechanizmów.

4. Urządzenia dostępowe dla urządzeń serwisowych (hala serwisowa w lokalizacji przy siedzibie głównej)

a) Zakres radiowy : 1 x 2.4 GHz single-band oraz 1 x 5 GHz single-band
b) Zakres Wi-Fi: Wi-Fi 6
c) Certyfikaty jakie musi posiadać urządzenie: CB, UL, CE, FCC, ISED, RCM, TEC
d) Urządzenie sieciowe musi być tego samego producenta co Firewall
e) Gwarancja 36 miesięcy

5. Szkolenia administratorskie - minimalny zakres tematyczny szkoleń:

Szkolenie administratorskie musi zawierać omówienie takich obszarów jak:

a. Wprowadzenie do firewalli:
   - Podstawowe pojęcia i definicje (firewall, strefa DMZ, NAT, filtracja pakietów, stanowa inspekcja).
   - Znaczenie i rola firewalli w ochronie sieci.
b. Architektura i komponenty systemu:

- Przegląd architektury typowego rozwiązania firewall.
- Opis komponentów systemu firewall i ich roli (interfejsy, reguły, polityki).
- Schematy sieciowe i topologie z uwzględnieniem firewalli.

c. Instalacja i konfiguracja:
   - Wymagania systemowe i przygotowanie środowiska.
   - Procedury instalacji sprzętowego i programowego firewalla.
   - Podstawowa konfiguracja firewalli (adresacja IP, interfejsy sieciowe, strefy bezpieczeństwa).

d. Konfiguracja polityk bezpieczeństwa:
   - Tworzenie i zarządzanie politykami bezpieczeństwa.
   - Ustawienia reguł pozwalających, blokujących i monitorujących ruch sieciowy.
   - Konfiguracja filtracji pakietów, filtrowanie aplikacji, inspekcja protokołów.

e. Zarządzanie użytkownikami i dostępem:
   - Konfiguracja kont użytkowników i uprawnień administratorów.
   - Mechanizmy autoryzacji i uwierzytelniania.
   - Zarządzanie rolami i dostępem do konsoli zarządzania firewall.

f. Monitorowanie i logowanie:
   - Narzędzia do monitorowania ruchu sieciowego i działania firewalla.
   - Analiza logów i generowanie raportów dotyczących aktywności i incydentów.
   - Konfiguracja systemów ostrzegania i powiadamiania o incydentach.

g. Zarządzanie zagrożeniami i incydentami:
   - Identyfikacja, analiza i reagowanie na zagrożenia oraz incydenty bezpieczeństwa.
   - Tworzenie i wdrażanie procedur zarządzania incydentami.
   - Integracja firewalla z systemami SIEM (Security Information and Event Management).

h. Aktualizacje i utrzymanie systemu:
   - Procedury aktualizacji oprogramowania i sygnatur bezpieczeństwa.
   - Regularne przeglądy i testy konfiguracji firewalli.
   - Tworzenie kopii zapasowych i planowanie odzyskiwania danych.

i. Zaawansowane funkcje i optymalizacja:
   - Wykorzystanie zaawansowanych funkcji firewalli nowej generacji (NGFW) takich jak IDS/IPS, filtrowanie URL, inspekcja SSL/TLS.
   - Optymalizacja wydajności firewalla.
   - Integracja z innymi systemami bezpieczeństwa (VPN, proxy, DLP).

j. Symulacje i scenariusze:
   - Ćwiczenia praktyczne z konfiguracji, monitorowania i reagowania na zagrożenia.
   - Scenariusze symulacji ataków i incydentów bezpieczeństwa.

k. Wsparcie techniczne i rozwiązywanie problemów:
   - Procedury identyfikacji i rozwiązywania najczęstszych problemów.
   - Korzystanie z dokumentacji, forum wsparcia i kontaktu z pomocą techniczną.

Załącznik nr 4 do zapytania ofertowego – Opis przedmiotu zamówienia

W zakresie ochrony poczty:

Szkolenie administratorskie musi zawierać omówienie takich obszarów jak:

a. Wprowadzenie do ochrony poczty:
   - Podstawowe pojęcia i definicje (spam, wirusy, spyware, phishing, malware).
   - Znaczenie i potrzeba ochrony poczty elektronicznej.
b. Architektura i komponenty systemu:
   - Opis i rola poszczególnych komponentów systemu ochrony poczty.
   - Schematy architektury systemu i przepływ poczty przez system ochrony.
c. Instalacja i konfiguracja:
   - Wymagania systemowe i przygotowanie środowiska.
   - Procedury instalacji oprogramowania ochrony poczty.
   - Konfiguracja podstawowych ustawień systemu.
   - Konfiguracja logów i backupów.
d. Konfiguracja polityk bezpieczeństwa:
   - Tworzenie i zarządzanie politykami antyspamowymi, antywirusowymi i antyspyware'owymi.
   - Ustawienia filtrów i reguł dotyczących różnych typów zagrożeń.
   - Konfiguracja list zaufanych i blokowanych nadawców (whitelisting i blacklisting).
e. Monitorowanie i zarządzanie zagrożeniami:
   - Narzędzia do monitorowania stanu ochrony i wykrywania zagrożeń.
   - Analiza logów i raportów dotyczących ataków i wykrytych zagrożeń.
   - Przykładowe procedury reagowania na incydenty bezpieczeństwa.
f. Aktualizacje i utrzymanie systemu:
   - Metody i harmonogramy aktualizacji sygnatur antywirusowych i antyspyware'owych.
   - Procedury aktualizacji oprogramowania i systemów.
   - Regularne przeglądy i testy systemu ochrony.
g. Zaawansowane funkcje i optymalizacja:
   - Wykorzystanie zaawansowanych funkcji ochrony, takich jak analiza heurystyczna, sandboxing, itd.
   - Optymalizacja wydajności systemu ochrony poczty.
   - Integracja z innymi systemami bezpieczeństwa i narzędziami.
h. Zarządzanie użytkownikami i dostępem:
   - Konfiguracja uprawnień użytkowników i administratorów.
   - Mechanizmy autoryzacji i uwierzytelniania.
   - Zarządzanie rolami i dostępem do systemu.
i. Symulacje i scenariusze:
   - Ćwiczenia praktyczne z konfiguracji, monitorowania i reagowania na zagrożenia.
   - Scenariusze symulacji ataków i incydentów bezpieczeństwa.
j. Wsparcie techniczne i rozwiązywanie problemów:

- Procedury identyfikacji i rozwiązywania najczęstszych problemów.
- Korzystanie z dokumentacji, forum wsparcia i kontaktu z pomocą techniczną.

6. Dokumentacja

Wykonawca przedstawi Zamawiającemu do akceptacji spis treści proponowanej dokumentacji, w zakresach:

- Dokumentacji przed wdrożeniowej,
- Dokumentacji po wdrożeniowej. Zakres dokumentacji ma umożliwiać osobie nieznającej produktu przywrócenie konfiguracji urządzenia.

7. Asysta

Wykonawca przeniesienie konfigurację z aktualnie posiadanych modeli urządzeń przez Zamawiającego, na nowe urządzenia oraz uruchomi nowo zakupione licencje , zgodnie z zamówionymi i dostarczonymi licencjami.