Załącznik Nr 1 do SWZ

Opis przedmiotu zamówienia

(Znak postępowania: **ZPF.271.20.2025**

Część 1:

a) „Wdrożenie i audyt SZBI czyli dokumentacji zgodnej z wymaganiami normy ISO 27001, mającej na celu zapewnienie wyższego poziomu bezpieczeństwa Urzędu Gminy i Miasta Rudnik nad Sanem”

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w odniesieniu do normy PN-EN ISO/IEC 27001 i wdrożenie narzędzia do prowadzenia procesu analizy ryzyka

W ramach prac Wykonawca zobowiązany jest do:

1. **Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w odniesieniu do normy PN-EN ISO/IEC 27001:**
   A. Przeprowadzenia inwentaryzacji aktywów oraz określenia wymagań realizacji audytu wstępnego. Wraz z identyfikacją aktywów oraz inwentaryzacją zasobów zostanie opracowana klasyfikacja wagi aktywów w odniesieniu do standardu bezpieczeństwa informacji.
   B. Przeprowadzenia audytu wstępnego, w którym przeprowadzi szczegółową analizę wdrożonej dokumentacji, procesów, polityk i procedur w organizacji. Analizie oprócz aspektów organizacyjnych należy poddać również systemy wchodzące w skład infrastruktury informatycznej w celu odniesienia wdrożonego standardu do możliwości technicznych. Wykonawca zidentyfikuje obszary wymagające usprawnienia oraz zaproponuje zmiany mające na celu poprawę standardu zarządzania bezpieczeństwem informacji w przedsiębiorstwie.
   C. Przygotowania polityk bezpieczeństwa informacji i procedur operacyjnych zgodnych ze zdefiniowanymi celami, zakresami i działalnością organizacji. Wykonawca przeprowadzi analizę posiadanej dokumentacji pod kątem zgodności z wytycznymi.

Usługa będzie realizowana we współpracy z Zamawiającym. Wykonawca na każdym etapie realizacji usługi będzie w stałym kontakcie z zespołem wdrożeniowym po stronie Zamawiającego.

W ramach dokumentacji zostaną opracowanie i uwzględnione poniższe obszary:

a. Kroki podjęte w celu zapewnienia bezpieczeństwa informacji, a w tym:
   i. Cele bezpieczeństwa informacji, sposoby ich realizacji i odpowiedzialność za nie,
   ii. Polityka Bezpieczeństwa informacji opracowana w oparciu o właściwe standardy i dobre praktyki,
   iii. Zdefiniowana procedura przeglądu PBI,
b. Zasady, procedury i procesy zarządzania, monitorowania wymogów w zakresie regulacyjnym, prawnym, ryzyka, ochrony środowiska i operacyjnym w organizacji, szacowanie i zarządzanie ryzykiem, tolerancja ryzyk operacyjnych oraz we współpracy zewnętrznej:
   i. Identyfikacja kluczowych aktywów informacyjnych Jednostki (tj. zbiory danych/systemy/usługi), rejestr ryzyk oraz procedury zarządzania ryzykiem
   ii. Identyfikacja podatności w środowisku Zamawiającego, szacowanie ryzyka związanego z zagrożeniami bezpieczeństwa informacji, identyfikacja zagrożeń zewnętrznych i wewnętrznych,
   iii. Klasyfikacja zagrożeń, podatności, prawdopodobieństwa ich wystąpienia i skutki,
   iv. Procedury oceny dostawców i partnerów zewnętrznych w celu zwiększenia bezpieczeństwa łańcucha dostaw

D. Przeprowadzenia kompleksowej analizy ryzyk i bezpieczeństwa systemów informatycznych w oparciu o gotowe, dedykowane do tego celu narzędzie informatyczne spełniające poniższe wymagania:

a. Narzędzie umożliwi prowadzenie, aktualizację oraz eksport wyników analizy ryzyka,
b. Pełny interfejs aplikacji w języku polskim,
c. Narzędzie może być obsługiwane z poziomu przeglądarki internetowej,
d. Komunikacja będzie odbywać się z wykorzystaniem bezpiecznego, szyfrowanego połączenia SSL,
e. Architektura aplikacji nie będzie wymagać od Zamawiającego zapewnienia dodatkowych zasobów sprzętowych oraz wydajnościowych,
f. Aplikacja będzie zapewniała minimum poniższe funkcjonalności:
    i. możliwość definicji różnych poziomów dostępu do danych,
    ii. powiadomienia uczestników analizy ryzyka o zbliżających się terminach i przypisanych do nich zadaniach,
    iii. powiadomienia w postaci wiadomości e-mail i systemowych,
    iv. gotowe słowniki czynności przetwarzania informacji dostosowane do organizacji,
    v. możliwość kategoryzacji ryzyk,
    vi. możliwość realizacji procesu analizy ryzyka dla całości organizacji oraz dla wybranych jednostek organizacyjnych w wybranych obszarach czynności przetwarzania ryzyka
    vii. możliwość automatycznego tworzenia podprocesów dla wybranych czynności przetwarzania analizy ryzyka dla każdej jednostki organizacyjnej,
    viii. możliwość generowania raportów z analizy wraz z informacjami nt. postępowania z ryzykiem,
    ix. możliwość zapisu wyników analizy ryzyka do pliku pdf i word
    x. moduł prowadzenia procesu zarządzania ryzykiem wraz z definicją i przydzieleniem zadań naprawczych do wybranych użytkowników systemu, możliwość weryfikacji postępów prac naprawczych oraz definicji ich skuteczności,
    xi. możliwość integracji z usługami katalogowymi Active Directory

2. <u>Narzędzie informatyczne do prowadzenia procesu analizy ryzyka</u>

W ramach dostarczonej licencji Zamawiający będzie posiadał dostęp do pełnej funkcjonalności oprogramowania w okresie minimum 12 miesięcy od zakończenia usługi wdrożenia SZBI.

Oprogramowanie zostanie udostępnione Zamawiającemu przez Wykonawcę w modelu usługowym (z ang. w modelu SaaS, Software as a Service).

Oprogramowanie oraz przetwarzane w nim dane będą udostępnione w bezpiecznym środowisku dedykowanym do świadczenia usług w modelu SaaS z zastosowanymi minimalnymi zabezpieczeniami:

- Bezpieczeństwo fizyczne zapewnione poprzez system wideomonitoringu, kontrolę dostępu oraz ochronę osobową,
- Redundantne zasilanie na każdym stopniu (bez pojedynczych punktów awarii), zasilanie każdego elementy DC realizowane minimum dwoma niezależnymi obwodami,
- Ochrona przed pożarem w postaci sytemu automatycznego gaszenia oraz systemu wczesnej detekcji dymu,
- Wysoka dostępność zasobów zapewniona poprzez zastosowanie architektury wysokiej dostępności (HA) oraz zwielokrotnione łącze dostępowe do sieci Internet dostarczone przez minimum 3 operatorów przy użyciu minimum dwóch niezależnych ścieżek,
- Ośrodek danych objęty ciągłym monitoringiem w zakresie parametrów środowiskowych, parametrów systemów przetwarzania oraz dostępności
- Ośrodek danych powinien posiadać certyfikację ISO/IEC 27018 (ochrona danych osobowych w chmurze) oraz ISO/IEC 27017 (bezpieczeństwo przetwarzania w modelu chmurowym,
- Wykonawca musi być właścicielem ośrodka danych

Audyt SZBI

Audyt SZBI powinien polegać na:

- Określeniu kryteriów audytu
- Przygotowaniu planu audytu
- Ocena dokumentacji SZBI
  - przegląd polityk, procedur, planów działania, regulaminów.
  - weryfikacja czy organizacja posiada wszystkie niezbędne dokumenty zgodne z regulacjami wewnętrznymi, prawem lub normami, które wdrażają.
  - przegląd rejestru incydentów oraz działa podjętych w przypadku zidentyfikowania incydentów bezpieczeństwa informacji
  - przegląd procedur/systemów zarządzania dostępem do systemów i infrastruktury
- Ocena zidentyfikowanych ryzyk
  - przegląd dokumentacji oceny ryzyka
  - przegląd ryzyk czy zostały odpowiednio zidentyfikowane i sklasyfikowane
  - przegląd procesu analizy ryzyka, monitorowania i planów postępowania z ryzykiem
- Audyt techniczny
  - przegląd systemów i infrastruktury (mogą być w tym testy penetracyjne)
  - przegląd procedur zarządzania podatnościami
  - przegląd procedur kontroli zabezpieczeń sieciowych
  - przegląd procedur kontroli dostępu (jeżeli takowa jest w budynku)
  - przegląd procedur na wypadek awarii

Audyt SZBI zostanie zrealizowany zgodnie z wytycznymi organów kontroli. Zespół audytorski jest zobowiązany do weryfikacji zgodności z innymi przepisami, a w tym min. RODO, NIS2, KSC. Powinien być przeprowadzony zgodnie z wytycznymi projektu Cyberbezpiecznego Samorządu.

b) „Szkolenie z obsługi UTM oraz zaawansowanych sposobów obrony sieci przed cyberatakami dla administratorów sieci w Urzędzie Gminy i Miasta, jednostek organizacyjnych oraz szkołach Istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach projektu grantowego”

Kompleksowy pakiet szkoleń dla Administratorów w zakresie wybranych i stosowanych w Urzędzie technologii i rozwiązań

W ramach zadania Wykonawca przeprowadzi 3 oddzielne i niezależne procesy szkoleniowe obejmujące poniższe zagadnienia.

1. **Certyfikowane szkolenie z cyberbezpieczeństwa**
   Szkolenie swoim zakresem powinno obejmować najnowsze i najlepsze rozwiązania w dziedzinie cyberbezpieczeństwa, w tym umiejętności związana z aktualnymi zagrożeniami, automatyzacją, podejściem zerowego zaufania, IoT, szacowania ryzyka. Minimalny zakres zagadnień podczas szkolenia:
   - Ogólne koncepcje bezpieczeństwa
   - Zagrożenia, podatności i środki zaradcze
   - Architektura zabezpieczeń

- Bezpieczeństwo operacyjne
- Zarządzanie bezpieczeństwem

Szkolenie powinno przygotowywać do certyfikacji międzynarodowym standardem potwierdzającym nabyte umiejętności, takie jak:

- Ocena stanu bezpieczeństwa środowiska organizacji i rekomendowanie oraz wdrażanie odpowiednich rozwiązań z zakresu bezpieczeństwa.
- Monitorowanie i zabezpieczanie hybrydowych środowisk, w tym chmury, urządzeń mobilnych, Internetu Rzeczy (IoT) i technologii operacyjnych (OT).
- Działanie z uwzględnieniem odpowiednich przepisów i polityk, w tym zasad ładu korporacyjnego, ryzyka i zgodności.
- Identyfikacja, analiza i reagowanie na zdarzenia i incydenty związane z bezpieczeństwem.

Po zakończeniu szkolenia, uczestnicy uzyskają imienny certyfikat potwierdzający ukończenie szkolenia oraz voucher uprawniający do podjęcia certyfikacji międzynarodowym standardem. Szkolenie powinno być dostępne zarówno w formie stacjonarnej jak i online, Zamawiający na etapie realizacji określi dogodną formę przeprowadzenia szkolenia.

2. **Szkolenie z technologii stosowanych w Urzędzie oraz dostarczanych w ramach postępowania**

Szkolenie swoim zakresem powinno obejmować wszelkie umiejętności niezbędne do zarządzania i administrowania systemem bezpieczeństwa dostarczanym w ramach postępowania, a w szczególności zasady stosowania zapory sieciowej, uwierzytelnianie użytkowników, wysoka dostępność, SSL VPN, site-to-site IPsec VPN oraz sposoby ochrony sieci za pomocą profili bezpieczeństwa takich jak IPS, antywirus, filtrowanie sieci, kontrola aplikacji i inne. Minimalny zakres zagadnień podczas szkolenia:

- Ustawienia systemowe i sieciowe
- Zasady zapory sieciowej i NAT
- Routing
- Uwierzytelnianie zapory sieciowej
- Pojedyncze logowanie (FSSO)
- Operacje na certyfikatach
- Antywirus
- Filtrowanie sieci
- Zapobieganie włamaniom i kontrola aplikacji
- SSL VPN
- IPsec VPN
- Konfiguracja i monitorowanie SD-WAN
- Security Fabic
- Wysoka dostępność
- Diagnostyka i rozwiązywanie problemów

Po zakończeniu szkolenia, uczestnicy uzyskają imienny certyfikat potwierdzający ukończenie szkolenia i nabyte umiejętności. Szkolenie powinno być realizowane przez certyfikowanych trenerów wybranych technologii i przyjmować formę zarówno wykładów teoretycznych jak i laboratoriów.

3. **Szkolenie teoretyczne, warsztaty techniczne i konsultacje w środowisku i infrastrukturze Urzędu w zakresie rozwiązań Windows Server oraz systemów ochrony stosowanych w organizacji**

Szkolenie swoim zakresem powinno obejmować technologie wykorzystywane na co dzień w Urzędzie oraz zapewniać wiedzę niezbędną do odpowiedniego zarządzania systemami operacyjnymi oraz środowiskiem domenowym Urzędu. Minimalny zakres zagadnień podczas szkolenia:

- Wprowadzenie do Windows Server

- Usługi Active Directory
- Usługi infrastruktury sieciowej (DHCP, DNS, VPN, IPAM)
- Zarządzanie pamięciami masowymi
- Wirtualizacja
- Bezpieczeństwo systemu
- Wysoka dostępność i odzyskiwanie danych
- Zdalne zarządzanie
- Monitorowanie środowiska i jego wydajności
- Aktualizacja i migracja systemu

W ramach szkoleń powinny także zostać przeprowadzone warsztaty techniczne realizowane w środowisku Urzędu obejmujące swoim zakresem minimum:

- Przygotowanie środowiska laboratoryjnego
- Instalacja i konfiguracja systemu
- Konfiguracja usług domenowych
- Wdrażanie GPO
- Konfiguracja usług sieciowych
- Konfiguracja wirtualizacji
- Wdrażanie usług pulpitu zdalnego
- Automatyzacja
- Monitorowanie i rozwiązywanie problemów

W ramach szkoleń Wykonawca zapewni wsparcie oraz konsultacje w ramach administrowanego systemu w zakresie nie mniejszym niż 20 godzin roboczych do wykorzystania w okresie 12 miesięcy od zakończenia procesu szkoleniowego. Wsparcie i konsultacje będą obejmować środowisko Urzędu oraz stosowane w nim technologie, prace rozwojowe oraz koncepcyjne związane z zapewnieniem cyberbezpieczeństwa w organizacji.

c) „Szkolenie z cyberbezpieczeństwa dla pracowników Urzędu Gminy i Miasta Rudnik nad Sanem, pracowników jednostek organizacyjnych oraz szkół powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami”

Badanie świadomości użytkowników końcowych i szkolenia z cyberbezpieczeństwa

Wykonawca wykona usługi z zakresu badania świadomości użytkowników, szkolenia z cyberbezpieczeństwa oraz weryfikacja nabytej wiedzy dla pracowników Zamawiającego oraz jednostek podległych w zakresie:

1. Zamawiający wymaga opracowania kampanii socjotechnicznej w formie symulowanego ataku dla pracowników Urzędu:
   a. Zamawiający dostarczy listę mailingową pracowników objętych badaniem.
   b. Wykonawca powinien przeprowadzić proces badania świadomości użytkowników przy użyciu spreparowanej wiadomości email symulującej prawdziwy atak phishingowy.
   c. Wiadomość email powinna nakłaniać pracowników do kliknięcia w link, który będzie prowadził do pustej strony WWW.
   d. Wykonawca powinien prowadzić ewidencję uwzględniającą liczbę kliknięć oraz pozwalać na identyfikację użytkownika bądź urządzenia z którego link został użyty.
   e. Ewidencja i wyniki badania powinny zostać dostarczone w formie raportu maksymalnie 2 tygodnie po zakończeniu procesu.
   f. Kampanie powinny zostać przeprowadzone przed szkoleniem opisanym w punkcie 2.
2. Zamawiający wymaga realizacji szkoleń z cyberbezpieczeństwa dla pracowników Urzędu i jednostek podrzędnych.

a. Sesja szkoleniowa powinna trwać maksymalnie 150 minut i powinna uwzględniać minimum jedną 15 minutową przerwę.
b. Szkolenie w formie stacjonarnej w siedzibie Zamawiającego.
c. Grupą docelową szkoleń będą pracownicy Zamawiającego korzystający z technologii informatycznych.
d. Zakres tematyczny szkolenia powinien obejmować minimum poniższe zagadnienia:
    i. Wprowadzenie do cyberbezpieczeństwa
    ii. Typy zagrożeń i najczęstsze sposoby ataków
    iii. Rola użytkownika w bezpieczeństwie
    iv. Podpis cyfrowy
    v. Uwierzytelnianie i autoryzacja
    vi. Poczta elektroniczna
    vii. Bezpieczeństwo w Internecie
    viii. Bezpieczeństwo sieci bezprzewodowej
    ix. Bezpieczeństwo urządzeń mobilnych
    x. Bezpieczeństwo w mediach społecznościowych
    xi. Postępowanie w przypadku naruszenia bezpieczeństwa
    xii. Analiza przypadków zgłoszonych przez użytkowników
e. Wykonawca udostępni materiały szkoleniowe bezpośrednio po zakończeniu sesji szkoleniowych.
f. Szkolenie powinno przyjąć formę wykładu wraz z prezentacją.
g. W ramach sesji szkoleniowej uczestnicy mają możliwość prowadzenia dyskusji z trenerem oraz zadawania pytań.
h. Wymaga się pokazu „na żywo" działającego systemu ochrony firewall z omówieniem logów oraz pokazem przykładowych reguł ochrony.
i. Jedna grupa szkoleniowa nie powinna przekraczać **20 osób**.
j. Całkowita liczba pracowników objętych szkoleniem: **200 osób**.
k. Zamawiający wymaga opracowania harmonogramu szkoleń umożliwiającego udział w sesji szkoleniowej każdemu pracownikowi.
l. Sesje powinny być zrealizowane w ciągu nie więcej niż 2 tygodni kalendarzowych, zgodnie z harmonogramem szkoleń ustalonym przez Strony,
m. Po zakończeniu szkoleń przeprowadzona zostanie dodatkowa weryfikacja wiedzy pracowników w formie testu wiedzy dostępnego online.

Wyniki testu wiedzy powinny zostać dostarczone w formie raportu maksymalnie 2 tygodnie po zakończeniu procesu.

Część 2:
„Dostawa i wdrożenie sprzętowego firewalla (urządzeń typu UTM) do szkół oraz OPS, ZEAS i Zakładu Gospodarki Komunalnej w Rudniku nad Sanem"

Modernizacja systemu bezpieczeństwa w jednostkach podległych

W ramach projektu należy przeprowadzić modernizację systemu bezpieczeństwa w jednostkach podległych.

W ramach prac należy dostarczyć urządzenie umożliwiające **wdrożenie systemu bezpieczeństwa brzegu sieci.** Na dostarczanym urządzeniu należy wyznaczyć strefy bezpieczeństwa zgodnie z wymaganiami Zamawiającego a w szczególności strefy:

- WAN – strefa przeznaczona do podłączenia łącza internetowego
- LAN – strefa przeznaczona dla użytkowników oraz serwerów

W zakresie Wykonawcy jest również wykonanie pełnej konfiguracji zapory sieciowej zgodnie z dobrymi praktykami bezpieczeństwa oraz przeniesienie konfiguracji z istniejących już urządzeń jeśli będzie to wymagane. Dodatkowo należy wykonać połączenia VPN Site-to-Site oraz klienckie w ustaleniu z

Zamawiającym. Wykonawca zobowiązany jest do konfiguracji nowo dostarczanych urządzeń oraz istniejących pod nadzorem administratorów. Podczas wdrożenia Zamawiający może wprowadzić zmiany w wymaganej konfiguracji urządzeń i systemów.

Dla szkół (5) należy dostarczyć urządzenie klasy UTM spełniające poniższe wymagania:

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.

5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).

- Microsoft Azure.
- Cisco ACI.
- Google Cloud Platform (GCP).
- OpenStack.
- VMware NSX.
- Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).

7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
6. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
6. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

b) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięce

g) Logowanie, korelowanie zdarzeń, raportowanie oraz generowanie powiadomień w oparciu o usługę realizowaną w chmurze, na okres 24 miesięcy

Gwarancja oraz wsparcie

1. System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Dla pozostałych jednostek podległych (3) należy dostarczyć urządzenie klasy UTM spełniające poniższe wymagania:

Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: ○ Firewall. ○ Ochrony w warstwie aplikacji. ○ Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: ○ 5 portami Gigabit Ethernet RJ-45.

	2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.
Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: ○ Translację jeden do jeden oraz jeden do wielu. ○ Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

	3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. ○ Amazon Web Services (AWS). ○ Microsoft Azure. ○ Cisco ACI. ○ Google Cloud Platform (GCP). ○ OpenStack. ○ VMware NSX. ○ Kubernetes.
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: ○ Wsparcie dla IKE v1 oraz v2. ○ Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). ○ Obsługa protokołu Diffie-Hellman grup 19, 20. ○ Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. ○ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. ○ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. ○ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. ○ Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. ○ Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. ○ Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. ○ Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. ○ Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: ○ Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. ○ Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

	○ Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi

	serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące

	źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

	6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	Wymaga się dostawy urządzenia wraz ze wsparciem producenta uprawniającym do korzystania z aktualnych baz funkcji ochronnych: • Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.
Gwarancja oraz wsparcie	System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.