

## **OPIS PRZEDMIOTU ZAMÓWIENIA**

**„Dostawa i konfiguracja Firewall next-generation w Urzędzie Gminy Zielonki w ramach projektu  
Cyberbezpieczny Samorząd”**

**Zamawiający:**

**Gmina Zielonki**

## **DOSTAWA INFRASTRUKTURY SPRZĘTOWEJ ORAZ OPROGRAMOWANIA**

Przedmiotem zamówienia jest dostawa sprzętu i oprogramowania podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych w urzędzie gminy Zielonki

Poniżej wyspecyfikowano minimalne parametry sprzętu oraz oprogramowania, które należy dostarczyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

Wymagania ogólne:

- Całość dostarczanego sprzętu standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
- Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, musi być nowe, wcześniej nieużywane, rok produkcji nie starszy niż 2024.
- Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, w którym nie wskazano szczegółowych warunków gwarancji, musi być objęte minimum 24 miesięczną gwarancją jeśli w opisie parametrów nie wskazano inaczej
- Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
- Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
- Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
- Wszystkie urządzenia muszą posiadać oznakowanie CE.
- Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
- Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V  $\pm$  10%, 50 Hz.
- Wymagane jest, aby infrastruktura sprzętowa była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.

### **Opis parametrów minimalnych dostarczanej infrastruktury oraz oprogramowania:**

Wymagania dla Wykonawcy który dostarczy infrastrukturę sprzętową oraz oprogramowanie:

Zamawiający wymaga, aby Wykonawca spełniała wymagania w zakresie:

## Zestawienie wymaganego sprzętu i oprogramowania

Lp.	Typ sprzętu	Ilość
1.	Firewall next-generation	3 szt.

Firewall next-generation – 3 szt.

Nazwa producenta: .....

Nazwa i typ: .....

1.	System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Akceptowana jest również separacja logiczna zasobów zrealizowana za pomocą przypisania dedykowanej ilości rdzeni zasobów procesorów (tzw. CPU cores) do obu z funkcji lub alternatywnie za pomocą oddzielnych dedykowanych procesorów (tzw. CPU) dla każdej z funkcji. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta
2.	Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta. Producent oferowanego rozwiązania w postępowaniu był wskazywany w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części („ćwiartce) Leaders w co najmniej jednym raporcie opublikowanym w ciągu ostatnich 18 miesięcy liczonym od terminu składania ofert.
3.	System zabezpieczeń firewall musi posiadać przepływność nie mniej niż 2,6 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 1,2 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS) i obsługiwać nie mniej niż 195 000 jednoczesnych połączeń oraz 34000 nowych sesji na sekundę.
4.	System zabezpieczeń firewall musi posiadać konstrukcję bez wentylatorową oraz być wyposażony w co najmniej 8 portów tzw. "miedzianych" 1G, dedykowany port do zarządzania 1G oraz port konsolowy RJ45 lub micro USB.
5.	Interfejsy sieciowe systemu zabezpieczeń firewall muszą działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA
6.	Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a system zabezpieczeń firewall musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
7.	System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Interfejsy sieciowe pracujące w trybie transparentnym, L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać 4000 znaczników VLAN

8.	System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
9.	Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie
10.	System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
11.	System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
12.	Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.
13.	Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).
14.	Nie jest dopuszczalne, aby blokowanie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
15.	Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
16.	System zabezpieczeń firewall musi wykrywać co najmniej 3500 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. oraz z aplikacjami przemysłowymi (tzw. ICS/OT) np. DNP3, Modbus.
17.	System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
18.	System zabezpieczeń firewall musi zapewniać możliwość segmentacji aplikacji na standardowych dla nich portach usług w obrębie pojedynczej reguły polityki firewall, tj. musi istnieć możliwość takiej konfiguracji pojedynczej reguły firewall, która zezwoli na działanie kilku aplikacji, wyłącznie jeśli nawiązanie połączenia następuje na port właściwy dla danej aplikacji, np. jeśli pojedyncza reguła zezwala na ruch SMTP i DNS, to SMTP nie może być dozwolone na porcie 53 (właściwym dla DNS), a DNS na porcie 25 (właściwym dla SMTP).
19.	System zabezpieczeń firewall musi automatycznie weryfikować spójność konfiguracji polityk bezpieczeństwa z punktu widzenia kompletności użytych przez administratora sygnatur aplikacyjnych potrzebnych do prawidłowego działania polityki. Np. jeśli do prawidłowej obsługi dostępu do aplikacji „Facebook” potrzebne jest dodatkowo użycie aplikacji „SSL”, a administrator nie uwzględni tej aplikacji w polityce, to system

	powinien ostrzec o tym fakcie administratora w momencie zatwierdzania nowej polityki.
20.	System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
21.	System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
22.	System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
23.	System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołami SSL/TLS 1.3 oraz HTTP/2) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i anyspyware), filtracja plików, danych i URL.
24.	System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
25.	System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
26.	System zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę aplikacji dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
27.	System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
28.	System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, serwerami

	Terminal Services). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmienia lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
29.	System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesję w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.
30.	Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.
31.	System zabezpieczeń firewall musi posiadać moduł analizujący, w czasie rzeczywistym, zapytania DNS przechodzące przez urządzenie w celu wykrywania domen złośliwych, domen generowanych przez algorytmy DGA oraz tunelowania złośliwej komunikacji (lub wycieku danych) w protokole DNS. Baza domen DNS-owych musi być regularnie aktualizowana w sposób automatyczny. Dodatkowo ochrona DNS powinna działać dla ruchu przechodzącego przez system zabezpieczeń firewall bez potrzeby wskazywania go jako serwer DNS.
32.	System zabezpieczeń firewall musi posiadać możliwość kategoryzowania ruchu DNS i budowania reguł filtrujących wybrane kategorie w zależności od ryzyka z nimi związanego. System powinien rozróżniać co najmniej następujące kategorie domen: C&C, złośliwe, DDNS, nowo zarejestrowane, phishing.
33.	System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
34.	System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny.
35.	System zabezpieczeń firewall musi umożliwiać kategoryzację strony WWW za pomocą mechanizmu przypisującego do konkretnej strony kilka kategorii (np. portal finansowy i portal informacyjny). Dodatkowo, powinna istnieć możliwość budowania własnych kategorii bazujących na kombinacji kategorii standardowych (np. własna kategoria wiadomości finansowe zawierające wszystkie strony skategoryzowane jako portale finansowe i informacyjne) jak również budowanie kategorii na bazie ryzyka bezpieczeństwa danej strony (niskie, średnie, wysokie) i określenia czy dana strona jest stroną nowopowstałą.
36.	System zabezpieczeń firewall musi posiadać mechanizm analizy w czasie rzeczywistym stron WWW i na podstawie algorytmów uczenia maszynowego rozpoznawać i

	blokować złośliwą zawartość JavaScript, złośliwe pliki wykonywalne (tzw. PE i DLL), złośliwe skrypty PowerShell, ataki Phishing jak również próby wykradania poświadczeń.
37.	System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
38.	System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
39.	System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
40.	System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekodery taki jak http, http2 smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
41.	Rozwiązanie musi posiadać możliwość analizy, identyfikacji oraz blokowania wcześniej nieznannej komunikacji C2 (command-and-control) oraz spyware w oparciu o mechanizmy uczenia maszynowego realizowane w chmurze producenta. Wymagana analiza i detekcja musi umożliwiać blokowanie wykrytej komunikacji C2 w czasie rzeczywistym). Analiza i wykrywanie nieopisanych wcześniej w sygnaturach połączeń C2 musi być możliwa minimum dla ruchu typu: http, http2, ssl, niezidentyfikowanych przez firewall aplikacji działających na protokołach TCP i UDP. Aktualizacja zasad i sposobu pracy silników detekcji, powinna być realizowana w chmurze producenta bez potrzeby aktualizacji oprogramowania i instalacji nowych wersji reguł i sygnatur na firewallu zaimplementowanym w chronionym środowisku.
42.	System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduł inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
43.	System zabezpieczeń firewall musi posiadać moduł wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
44.	System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
45.	System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

46.	System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
47.	System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
48.	System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
49.	System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
50.	System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
51.	System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW oraz kategorii URL, serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany.
52.	System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
53.	System zabezpieczeń firewall musi posiadać funkcję wykrywania na podstawie algorytmów uczenia maszynowego złośliwych plików wykonywalnych, skryptów PowerShell oraz plików MS Office przechodzących przez urządzenie i blokowania ich w czasie rzeczywistym.
54.	System bezpieczeństwa musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznego systemu typu „Sand-Box” (np. dostarczanego przez producenta zaoferowanego Systemu) plików wykonywalnych (minimum pliki typu PE) i dokumentów (minimum MS Office i PDF) przechodzących przez firewall w celu ochrony przed zagrożeniami typu zero-day. System zewnętrzny, na podstawie przeprowadzonej analizy, musi aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.
55.	Administrator musi mieć możliwość konfiguracji mechanizmu wysyłania plików wykonywalnych (minimum pliki typu PE) i dokumentów (minimum MS Office i PDF) do

	środowiska chmurowego producenta typu „Sand-Box”, zaoferowanego systemu w celu wykrywania potencjalnych nierozpoznanych sygnaturowo zagrożeń.
56.	Administrator musi posiadać możliwość zdefiniowania jaki rodzaj plików będzie wysyłany do „Sand-Box-a” i w jakiej relacji ruchowej (download, upload).
57.	Administrator musi mieć możliwość dostępu do systemu analizy plików wykonywalnych w celu sprawdzenia, które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.
58.	System „Sand-Box” działający po stornie producenta, musi zwrotnie przysyłać aktualizacje sygnatur wykrytych zagrożeń, z częstotliwością jaką zapewnia producenta dla działania tego mechanizmu
59.	Urządzenia firewall muszą obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
60.	Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa.
61.	Wykonywanie operacji deszyfrowanie ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji. Musi zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.
62.	Dla deszyfrowania ruchu TLS 1.3 wymagane jest wsparcie dla X25519, X448 oraz minimum dla zestawów protokołów: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384 oraz TLS_CHACHA20_POLY1305_SHA256.
63.	System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
64.	System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
65.	System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
66.	System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN).
67.	System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentication) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, SAML 2.0.

68.	System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ
69.	Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
70.	Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
71.	System zabezpieczeń firewall musi posiadać wbudowany dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 128GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
72.	Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW przez dedykowany interfejs do zarządzania lub inny interfejs wypromowany jako interfejs zarządzający. Nie jest dopuszczalne, aby istniała konieczność instalacji lub pobierania dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
73.	Urządzenia firewall muszą posiadać koncept konfiguracji kandydackiej (na poziomie API, GUI, oraz CLI), którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.
74.	Konfiguracja kandydacka musi być wspierana przez minimum 7 dni. W tym: <ul style="list-style-type: none"> <li>a. Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalając im na zatwierdzanie i cofanie zmian, których są autorami.</li> <li>b. Możliwość blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji</li> </ul>
75.	System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
76.	Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
77.	System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+
78.	System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
79.	System zabezpieczeń firewall musi posiadać mechanizm umożliwiający wysyłanie logów do zewnętrznego kolektora danych
80.	System zabezpieczeń firewall musi posiadać mechanizm umożliwiający monitorowanie stanu urządzenia z wykorzystaniem SNMP v2 i v3

81.	System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
82.	System zabezpieczeń firewall musi zapewniać mechanizm pozwalający na sprawdzenie podczas procesu instalacji nowej bazy sygnatur aplikacyjnych, które reguły bieżącej polityki bezpieczeństwa wykorzystują sygnatury aplikacyjne modyfikowane w ramach bieżącej aktualizacji baz sygnatur.
83.	System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.
84.	System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
85.	System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
86.	System zabezpieczeń firewall musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.
87.	System zabezpieczeń firewall musi pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
88.	System zabezpieczeń firewall musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
89.	System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
90.	Elementy do montażu w szafie rack
91.	Wykonawca zapewni usługi wdrożeniowe w następującym zakresie: <ul style="list-style-type: none"> <li>a. W ramach wdrożenia Wykonawca dokona instalacji fizycznej w miejscu wskazanym przez zamawiającego, aktualizacji oprogramowania dostarczonych urządzeń do wersji oprogramowania rekomendowanej przez producenta a następnie konfiguracji nowych urządzeń na podstawie konfiguracji urządzeń aktualnie wykorzystywanych przez Zamawiającego wraz z przeniesieniem reguł bezpieczeństwa i konfiguracji uruchomionych funkcjonalności urządzeń (jeśli dotyczy). Odbiór migracji zostanie poprzedzony testami opracowanymi wraz z Zamawiającym w zakresie spełnienia oczekiwanych funkcji.</li> <li>b. Po zakończonym procesie migracji Zamawiający dokona weryfikacji konfiguracji pod kątem bezpieczeństwa oraz elementów nadmiarowych. Zamawiający oczekuje wprowadzenia rekomendacji producenta w zakresie najlepszych praktyk w zakresie polityk i wykorzystywanych mechanizmów bezpieczeństwa.</li> </ul>
92.	Gwarancja 12 miesięcy