## 

## 

**Załącznik Nr 4**

Zamawiający : Miasto Czeladź, ul. Katowicka; Czeladź 41-250

Nr referencyjny postępowania: **SE-ZP. 271.1.1110.2024**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

1. Przedmiotem zamówienia jest dostawa wraz z wdrożeniem urządzenia UTM (wersja sprzętowa) typu zapora sieciowa nowej generacji (NGFW), która będzie w pełni kompatybilna i będzie stanowić element budowy klastra wysokiej dostępności HA z posiadanym przez Zamawiającego urządzenie Barracuda Cloud Gen Firewall F380.
2. Oferowany NGFW musi posiadać minimum następujące pakiet subskrypcji i realizować minimum następujące funkcjonalności:
3. 24-miesięczna subskrypcją na aktualizację w zakresie minimum: systemu operacyjnego urządzenia, aktualizację sygnatur dla silnika IPS, aktualizację sygnatur dla silnika dynamicznego rozpoznawania aplikacji.
4. 24-miesięczna subskrypcją na ochronę antywirusową w zakresie minimum: aktualizacje sygnatur silnika antywirusowego, sygnatur spamu oraz dostępu do serwerów RBL DNS.
5. 24-miesięczna subskrypcją na poszerzoną ochronę z wykorzystaniem technologii Sanboxingu, w zakresie minimum : zawansowanej analizy załączników, ochroną przed zagrożeniami dnia zerowego, ochrona przed atakami typu ransomware.
6. 24-miesięczna subskrypcją na Barracuda Control Center w modelu usługowym z dedykowanym zdalnym wsparciem technicznym minimum 2h w miesiącu lub równoważny tzn.: centralna udostępniona w chmurze platforma zarządzania wieloma urządzeniami klasy UTM w tym klastrem HA z różnymi narzędziami automatyzacji, takimi jak repozytorium, szablony i interfejsy API. Dostarczone w ramach platformy narzędzia muszą umożliwiać administratorom między innymi: monitorowanie stanu sieci, zarządzanie zestawami reguł zapory i zasadami bezpieczeństwa oraz wdrażanie poprawek oprogramowania i uaktualnień wersji. Platforma zarządzania musi być dostarczona w modelu usługowym, bez instalacji komponentów czy jakiegokolwiek oprogramowania w siedzibie Zamawiającego z wykorzystaniem jego infrastruktury sprzętowej. (warunki techniczne równoważności patrz pkt.4 ppkt 12. Zarządzanie urządzeniami klastra HA typu Firewall, realizowane przez centralną konsolę administracji i zarządzania…)
7. 24-miesięczna subskrypcją na rozszerzona gwarancję sprzętową Instant Repleacment lub równoważną (warunki równoważności patrz pkt. 6. Gwarancja i wsparcie techniczne producenta)
8. Oferowany w ramach postępowania sprzęt musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego producenta w Polsce. Sprzęt musi posiadać polskojęzyczne wsparcie techniczne.
9. **Wraz z dostawą UTM Zamawiający oczekuje wykonania usług przez Oferenta:**
10. *Wdrożenie, polegające na:*
11. Wykonawca zobowiązuje się do wdrożenia usług w lokalizacji Zamawiającego:
    * Wykonania uruchomienia Klastra HA.
    * Dodanie do konfiguracji zapasowego łącza internetowego oraz uruchomienia usługi SD-WAN w oparciu o dwa dostępne łącza internetowe.
    * Przeglądu obecnej konfiguracji UTM i ewentualnej rekonfiguracji o ustawień UTM w oparciu o tzw. najlepsze praktyki. Zakres rekonfiguracja musi odbyć się w uzgodnieniu z Zamawiającym.
12. Wdrożenie musi być wykonane przez polskojęzycznego inżyniera na poziomie Professional który posiada certyfikacje: CGF01, CGF02, CGF03, CGF04 lub równoważne.
13. W przypadku zaoferowania urządzeń równoważnych wdrożenie klastra musi być przeprowadzone przez polskojęzycznego inżyniera posiadającego maksymalny poziom certyfikacji udostępnianej przez producenta danego rozwiązania. Na życzenie Zamawiającego wykonawca udokumentuje posiadane umiejętności. W przypadku zaoferowania urządzeń równoważnych zakres wdrożenia zostaje rozszerzony do uruchomienia wszystkich funkcjonalności i polityk stosowanych przez Zamawiającego.
14. Wdrożenie zostanie wykonane kierując się zasadą utrzymania ciągłości dotychczas dostępnych usług u Zamawiającego. Dopuszcza się możliwość odejścia od tej zasady z zastrzeżeniem każdorazowego uzgadniania z Zamawiającym.
15. Szkolenie *-* Wykonawca dostarczy Zamawiającemu szkolenie CGF przypominające dla 3 administratorów Zamawiającego wraz z omówieniem nowych funkcji oprogramowania 9.0.x. Szkolenie musi być przeprowadzone w siedzibie Zamawiającego w wymiarze czasowym minimum 8h w terminie uzgodnionym z Zamawiającym.

W przypadku zaoferowania urządzeń / rozwiązania równoważnego Wykonawca zobowiązany jest do przeprowadzenia całej ścieżki szkoleniowej producenta dla 3 administratorów Zamawiającego w terminach uzgodnionych z Zamawiającym.

1. Dokumentacja - Wykonawca wykona dokumentację po-wdrożeniową z zakresu wykonanych prac instalacyjno-wdrożeniowych i dostarczy / udostępni w wersji (elektronicznej) Zamawiającemu w terminie do 7dni roboczych od zakończenia wdrożenia. W przypadku zaoferowania urządzeń / rozwiązania równoważnego Wykonawca zobowiązany jest do wykonania kompletnej dokumentacji wdrożeniowej w związku ze zmianą rozwiązania technologicznego i konfiguracją urządzeń od podstaw.

#### Licencje - wszystkie dostarczone licencje w ramach rozwiązania muszą obejmować wymagany okres minimum 24-miesięcy i nie mogą posiadać limitu użytkowników.

Wraz z urządzeniem wykonawca dostarczy wymagane do prawidłowej pracy licencje:

* 24-miesięczna subskrypcją na aktualizację: systemu operacyjnego urządzenia, aktualizację sygnatur dla silnika IPS, aktualizację sygnatur dla silnika dynamicznego rozpoznawania aplikacji.
* 24-miesięczna subskrypcją na ochronę antywirusową, aktualizacje sygnatur spamu oraz dostęp do serwerów RBL DNS.
* 24-miesięczna subskrypcją na poszerzoną ochronę z wykorzystaniem technologii Sanboxingu, w zakresie zawansowanej analizy załączników, ochrony przed zagrożeniami dnia zerowego oraz ochrony przed atakami typu ransomware.

#### Gwarancja i wsparcie techniczne producenta - Minimum 24-miesięczną gwarancja producenta obejmująca wszystkie elementy urządzenia zapewniająca w przypadku awarii wysłanie sprawnego sprzętu na wymianę na następny dzień roboczy od momentu zgłoszenia do serwisu producenta. Wymagany poziom serwisu SLA minimum 8x5xNBD

Gwarancja musi zapewniać również dostęp do poprawek oprogramowania oraz wsparcia technicznego producenta z czasem reakcji nie dłuższym niż 2 godziny od momentu zgłoszenia problemu. Wymagana jest dostępność usługi w trybie 8x5 w godzinach od 8:00 do 17:00 (e-mail; telefon)

Po upływie co najwyżej 4 lat Zamawiający musi posiadać możliwość nieodpłatnej wymiany sprzętu na fabrycznie nowe urządzenie w aktualnej (na moment wymiany) wersji sprzętowej w ramach tej samej serii/linii produktowej.

1. Oferowany Firewall klasy NGF musi spełniać następujące minimalne wymagania:

System bramy sieciowej typu Full State Inspection Firewall, rozwiązanie typu NGF F380 lub równoważne, które będzie pracowało jako jedno z urządzeń klastra HA w topologii wdrożeniowej „Active-Passive” powinno spełniać niżej wymienione wymagania będące jednocześnie kryteriami równoważności:

Kryteria równoważności:

1. Wymagana wydajność urządzenia:

* tryb Stateful Firewall minimum - 8,5 Gbps
* VPN (klucz szyfrujący 128 bitowy lub dłuższy) minimum 2,1 Gbps
* tryb z włączonym modułem IPS minimum - 2,5 Gbps
* tryb Next Generation Firewall minimum- 2,0 Gbps
* tryb Threat Protection minimum - 1,7 Gbps
* liczba równoległych sesji co najmniej - 400 000

1. Parametry urządzenia, interfejsy i zasilanie:

* Liczba interfejsów Ethernet 10/100/1000 BaseT minimum: 8
* Liczba interfejsów 10 GbE SFP+ minimum: 2
* Zasilanie: minimum jeden zasilacz wbudowany
* System mocowania w standardowej szafie 19-calowej – maksymalnie: 1U

1. Firewall (zapora bezpieczeństwa sieciowego pracująca w chmurze) powinna realizować minimum następujące funkcje ochronne:

* Firewall sieciowy: obsługa reguł segmentacji sieci na podstawie adresów IP i portów
* Firewall applikacyjny: obsługa reguł segmentacji na podstawie rozpoznanych aplikacji, z możliwością rezerwacji i ograniczenia pasma niezależnie dla obu kierunków ruchu
* System filtracji URL: obsługa reguł filtrujących adresy stron WWW w oparciu o kategorie i indywidualne adresy, z możliwością rezerwacji i ograniczenia pasma niezależnie dla obu kierunków ruchu
* System inspekcji ruchu zaszyfrowanego protokołem SSL: inspekcja ruchu przychodzącego i wychodzącego za pomocą reguł Application Control, URL Filtering
* System IPS (*Intrusion Prevention System*): filtrowanie ruchu pod kątem ataków typu *intrusion*
* System identyfikacji osób pracujących w sieci (*User Awareness*): współpraca z systemami przechowującymi informację o tożsamości osób korzystających z sieci: Active Directory, LDAP, Radius, TACACS+, X509, RSA Secure ID, SAML, lokalna baza użytkowników
* System wykrywania i blokowania botów i oprogramowania szpiegującego: filtracja ruchu zidentyfikowanego jako ruch *botnet/spyware*
* System filtrowania zawartości transmitowanych plików: możliwość filtrowania w oparciu o zawartość plików (np. pliki muzyczne/pliki audio), w oparciu o nazwę plików (wzorce nazw plików do odfiltrowania), w oparciu o typy mime transmitowanych plików
* System zarządzania równoległymi łączami do Internetu: możliwość konfiguracji polityki wykorzystania równoległych łączy do Internetu za pomocą reguł sieciowych lub aplikacyjnych
* System zarządzania pasmem łącza internetowego (*traffic shaping*): możliwość definicji pasma gwarantowanego, dostępnego i rezerwowanego za pomocą reguł sieciowych lub aplikacyjnych
* System wykrywania ataków zero-day, zamaskowanego oprogramowania typu Ransomware, zaawansowanej analizy załączników, wykorzystujące odseparowane środowisko do analizy zagrożeń typu Sandbox
* System budowy wirtualnej sieci prywatnej (VPN) typu *site-to-site*
* System budowy sieci typu SD-WAN (*Software Defined WAN*):
  + obsługa i szyfrowanie ruchu na co najmniej 8 równoległych połączeniach między węzłami SD-WAN (tunel VPN musi obsługiwać co najmniej 8 równoległych łączy TCP/IP)
  + obsługa reguł kierowania ruchu do równoległych łączy z uwzględnieniem co najmniej: dostępności łącza, przepustowości łącza, opóźnienia łącza, obciążenia i zmiany parametrów łącza z monitorowaniem dynamicznym
  + obsługa reguł kierowania ruchu do najkorzystniejszego w danej chwili połączenia
* System budowy wirtualnej sieci prywatnej (VPN) typu C*lient-to-Site*, czyli sieci zdalnego dostępu:
  + licencje dostarczone z urządzeniem nie mogą ograniczać liczby zainstalowanych klientów VPN
  + oprogramowanie klienta VPN dostosowane do systemów Windows, Linux, MAC OS, OpenBSD
  + system dostępu SSL VPN powinien obsługiwać hasła jednorazowe typu OTP (One Time Password), w szczególności powinien zapewniać pełną obsługę haseł Time-based One Time Password (TOTP)
* Systemy szyfrowania wykorzystywane w modułach VPN i SD-WAN certyfikowane zgodnie ze standardem FIPS 140-2
* Możliwość uruchomienia i konfiguracji systemów HTTP Proxy, Reverse Proxy, DHCP Server, SIP Proxy
* Obsługa i możliwość podłączenia do Microsoft Azure Virtual WAN
* Obsługa protokołów IPv4 i IPv6

1. Intrusion Prevention System (IPS):

* Moduł IPS „na urządzeniu” m.in. 10 000 sygnatur
* Wykrywanie oraz blokowanie szkodliwej zawartość w kodzie HTML oraz Javascript
* Inspekcja ruchu tunelowanego wewnątrz protokołu SSL, w zakresie analizy HTTPS, POPS oraz SMTPS
* Wykrywanie typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany
* Moduł skanujący działa na urządzeniu (firewall’u), bez potrzeby instalowania agenta na komputerach w sieci.
* Powiadamianie o wykrytych podatnościach w ruchu wraz z informacją o kodzie CV
* Konfiguracja jednego z trybów pracy modułu proaktywnej ochrony i inspekcji pakietów IPS w zakresie: tryb aktywny IPS, tryb passywny IDS; konfiguracja bazy wyjątków modułu IPS dla wybranych adresów IP (źródłowych i docelowych), portów docelowych; sygnatur bazy CVE

1. Kształtowanie pasma (Traffic Shapping):

* W oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma
* Ograniczenie pasma lub priorytetyzacja określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia z uwzględnieniem kierunku przesyłanych danych (upload / download) Kwalfikacja Traffic Shapping z uwzględnienim adresu IP (źródłowego i docelowego), portów docelowych; autoryzowanego użytkownika
* Tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring)
* Na podstawie aplikacji generującej ruch
* Traffic Shapping działa w oparciu o profile QoS Band tzw. klasyfikatory ruchu które są kolejkowane do fizycznych lub logicznych interfejsów firewall’a

1. Ochrona antywirusowa:

* Rozwiązanie ma umożliwiać inspekcję przez skaner antywirusowy, co najmniej jeden silnik antywirusowy powinien być dostarczony przez firmę inną niż producent rozwiązania
* Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
* Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji. Proponowany system powinien umożliwiać wysyłanie powiadomienia email o załączniku, który został zablokowany.

1. Wirtualne sieci prywatne (VPN):

* Wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) i site-to-site (lokalizacja-lokalizacja)
* Kanały VPN można budować w oparciu o PPTP VPN, L2TP VPN, Auto VPN, IPSec VPN, SSL VPN
* SSL VPN działa w trybach Tunel i Portal
* Funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover)
* Wsparcie dla technologii XAuth oraz Hub ‘n’ Spoke
* Tworzenie tuneli w oparciu o technologię Route Based
* Dedykowany klient IPSec VPN
* Multitransport VPN – tworzenie do 24 transportów w obrębie jednego tunelu VPN site-to-site pomiędzy tymi samymi lokalizacjami, korzystających z różnych łączy i ustawień
* Łączenie transportów VPN (agregacja łączy na poziomie pakietów, lub sesji) i wyznaczanie transportów zapasowych
* Kompresja i deduplikacja danych przesyłanych w tunelach VPN
* Buforowanie danych przesyłanych w tunelach VPN dla protokołów zdefiniowanych przez administratora

1. Filtr dostępu do stron WWW (URL filtering):

* Wbudowany filtr URL
* Działa w oparciu o klasyfikację URL zawierającą min. 80 kategorii tematycznych stron internetowych.
* Mechanizm białych i czarnych list bez limitu
* Wspierany przez HTTP PROXY, zgodny z protokołem ICAP w trybie REQUEST
* Definiowanie akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:
* blokowanie dostępu do adresu URL
* zezwolenie na dostęp do adresu URL
* blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora
* Strona blokady umożliwia wykorzystanie zmiennych środowiskowych
* Identyfikacja i blokowanie przesyłanych danych z wykorzystaniem typu MIME
* Tworzenie białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. Baza wyjątków tworzona przy użyciu dwóch metod:
* wskazanie/wpisanie docelowej domeny (np. \*.skype.com; \*.microsoft.com);
* wskazanie kategorii ruch (np. Bankowość i Finanse)
* Włączenia pamięci cache dla ruchu http
* Wbudowany i rekonfigurowany WEB portal powiadomień zwrotnych służący do informowania użytkowników o nałożonych restrykcjach/ograniczeniach wynikających z wdrożonej polityki bezpieczeństwa (np. zablokowanie strony WWW danego portalu z powodu niedozwolonej kategorii)

1. Uwierzytelnianie

* System uwierzytelniania użytkowników w oparciu o:
* lokalną bazę użytkowników
* zewnętrzną bazę użytkowników (zewnętrzny LDAP)
* usługę katalogową Active Directory
* zewnętrzną bazę użytkowników Radius; TACACS+
* integrację z usługę katalogową AZURE Active Directory
* Równoczesne użycie minimum 4 różnych baz LDAP
* Specjalny portal, który umożliwia autoryzacje w oparciu o protokoły:
* SSL
* Radius
* Kerberos
* Dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory
* Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.

1. Administracja łączami do Internetu (ISP):

Wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing)

* Mechanizm równoważenia obciążenia łącza internetowego działa w oparciu o następujące dwa mechanizmy:
* równoważenie względem adresu źródłowego
* równoważenie względem połączenia
* Mechanizm równoważenia łącza uwzględnia wagi przypisywane osobno dla każdego z łączy do Internetu
* Mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
* Mechanizm statycznego trasowania pakietów
* Trasowanie połączeń dla IPv6 w zakresie trasowania statycznego oraz mechanizmu przełączenia łącza zapasowego w przypadku awarii łącza podstawowego
* Trasowanie połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP
* Obsługa routingu dynamicznego w oparciu o protokoły: RIPv2, OSPF oraz BGP
* Wsparcie technologii Link Aggregation

1. Pozostałe usługi i funkcje rozwiązania:

* Wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci
* Przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay
* Konfiguracja serwera DHCP jest niezależna dla protokołu IPv4 i IPv6
* Tworzenie różnych konfiguracji dla różnych podsieci z możliwością określenia różnych bram, a także serwerów DNS
* Klient usługi SNMP w wersji 1,2 i 3
* Usługa DNS Proxy

1. Zarządzanie urządzeniami klastra HA typu Firewall, realizowane przez centralną konsolę administracji i zarządzania powinno posiadać następujące funkcje:

* konfiguracja urządzeń i polityki bezpieczeństwa za aplikacji graficznej działającej na komputerach z systemem Windows: ruch między stacją zarządzania i urządzeniem firewall powinien być zaszyfrowany
* możliwość równoległej pracy kilku administratorów
* możliwość konfiguracji dwóch urządzeń do pracy w klastrze HA (High Availability)
* możliwość konfiguracji dwóch urządzeń do pracy w klastrze geograficznie rozproszonym
* możliwość kopiowania konfiguracji elementów, reguł, obiektów pomiędzy urządzeniami (praca w trybie kopiuj-i-wklej)
* Obsługa protokołu monitorowania SNMP
* Obsługa protokołu monitorowania IPFIX
* Możliwość konfiguracji za pomocą REST API
* Obsługa przeglądania i filtrowania logów wbudowana w system Firewall
* Obsługa systemu zbierania statystyk do generowania raportów wbudowana w system Firewall

**UWAGA:**

W przypadku zaoferowania rozwiązania równoważnego Wykonawca na swój koszt wdroży i udowodni, że oferowane przez niego rozwiązanie jest nie gorsze niż posiadane obecnie przez Zamawiającego.

W przypadku zaoferowania rozwiązania równoważnego Wykonawca wykona kolejno w ramach złożonej oferty:

1. Kompleksowe szkolenie personelu IT w zakresie pełnej ścieżki szkoleniowej udostępnianej przez producenta rozwiązania – szkolenie i materiały w języku polskim, szkolenie w siedzibie Zamawiającego tj. 41-250 Czeladź, ul. Katowicka 45. Szkolenie powinno być dobrane pod względem liczby godzin tak aby w całości zabezpieczyć wiedzę na temat konfiguracji i administrowania oferowanym rozwiązaniem.
2. Dostawa urządzeń zgodnych z minimalnymi wymaganiami.
3. Kompleksowe wdrożenie nowego systemu w zakresie konfiguracji nie gorszym niż obecnie posiada Zamawiający w tym:

* Wykonanie uruchomienia Klastra HA
* Całkowitego odtworzenia wraz z przeglądem obecnej konfiguracji UTM wraz ewentualną rekonfiguracją ustawień UTM w oparciu o tzw. najlepsze praktyki. Zakres rekonfiguracja musi odbyć się w uzgodnieniu z Zamawiającym
* Dodanie do konfiguracji zapasowego łącza internetowego oraz uruchomienia usługi SD-WAN w oparciu o dwa dostępne łącza internetowe

dla urządzeń uruchomionych w siedzibie Zamawiającego z możliwością zarządzania lokalnie i zdalnie przez centralną platformę zarządzającą (należy uwzględnić również wdrożenie testowe).

1. Kompleksową dokumentacje po-wdrożeniową odzwierciedlającą cały proces konfiguracyjny wykonany na etapie produkcyjnego wdrożenia. Dokumentacja musi prezentować zakres przeprowadzonej konfiguracji, umożliwiać Zamawiającemu odtworzenie konfiguracji oraz zastosowanych polityk / reguł / zasad bezpieczeństwa na wypadek awarii.