Opis Przedmiotu Zamówienia
SPECYFIKACJA TECHNICZNA PRZEDMIOTU ZAMÓWIENIA

a) Sprzętowy serwer proxy WWW typu Secure Web Gateway – 1 szt.

Nazwa oferowanego sprzętu przez Wykonawcę (producent, typ/model):		
Lp.	Funkcje	Nazwa elementu, parametru lub cechy
1.	Założenia ogólne	Rozwiązanie sprzętowe – fizyczne urządzenie
		Obudowa typu 1U mini
		Minimalna przepustowość: 150Mbps.
		Minimalna wartość Web cache: 50GB
		Jednocześnie chronionych użytkowników: nie mniej niż 300
		Obsługa sieci wirtualnych (VLAN).
		Interfejs sieciowy: minimum 1 port 1Gb
		Dostępne złącza: VGA, PS/2 keyboard/mouse, port szeregowy (DB-9).
2.	Funkcjonalność ogólna	Urządzenie musi pracować przezroczyście (jako bridge) lub w trybie explicit proxy.
		Urządzenie musi posiadać możliwość współpracy z innymi urządzeniami/routerami w oparciu o protokół WCCP.
		Urządzenie musi obsługiwać filtrowanie ruchu http i https przesłanego do urządzenia przy pomocy protokołu WCCP.
		Urządzenie musi posiadać możliwość pracy w trybie audytu – monitorowanie oraz logowanie zdarzeń, lub w trybie aktywnym – filtrowanie ruchu wg definiowanych polityk oraz logowanie zdarzeń.
		Urządzenie musi pozwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: • lokalną bazę użytkowników, • zewnętrzną bazę użytkowników (zewnętrzny LDAP), • integrację z serwerem Microsoft Active Directory.
		Urządzenie musi pozwalać na jednoczesną autoryzację użytkowników z co najmniej dwóch różnych baz użytkowników.
		Aktualizacja firmware urządzenia musi być możliwa jest poprzez interfejs administracyjny.
		Urządzenie musi posiadać możliwość przywrócenia poprzednich zainstalowanych wersji firmware: możliwość przywrócenia do wcześniej zainstalowanej wersji firmware lub do wersji, która została zainstalowana fabrycznie.
		Urządzenie musi pozwalać na eksport/import konfiguracji poprzez interfejs administracyjny.
		Administrator musi posiadać możliwość wykonywania automatycznego eksportu konfiguracji na zewnętrzny serwer plików pracujący w oparciu o protokół FTP lub SMB.
		Urządzenie musi pozwalać na buforowanie zawartości stron na urządzeniu (Web cache).
		Administrator musi podsiadać możliwość wyłączyć Web cache dla wybranych domen.
3.	Filtrowanie ruchu	Urządzenie musi umożliwiać filtrowanie ruchu przy użyciu skanera antywirusowego dostarczonego wraz z urządzeniem. Uruchomienie skanera antywirusowego na urządzeniu nie może wymagać instalowania żadnej dodatkowej licencji.
		Producent musi dostarczyć wraz z urządzeniem aplikację kliencką służącą do wykrywania i usuwania złośliwego oprogramowania z komputerów klienckich.

		Dostarczona aplikacja nie może być limitowana na ilość komputerów, na których zostanie użyta.
		Urządzenie musi posiadać wbudowany filtr URL.
		Filtr URL musi działać w oparciu o klasyfikacje adresów URL dostarczoną przez producenta.
		Filtr URL musi zawierać co najmniej 95 kategorii tematycznych.
		Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.
		Baza adresów URL musi być przechowywana lokalnie w pamięci urządzenia.
		Administrator musi posiadać możliwość sprawdzenia z poziomu interfejsu administracyjnego do jakiej kategorii zaklasyfikowana jest strona.
		W przypadku strony nieskategoryzowanej administrator musi mieć możliwość zgłoszenia strony do kategoryzacji wraz z zaproponowaniem kategorii dla danej strony. Zgłaszanie strony do kategoryzacji ma odbywać się bezpośrednio z interfejsu administracyjnego.
		Administrator musi posiadać możliwość dodania własnej kategorii wraz z przypisanymi do niej domenami.
		Administrator musi podsiadać możliwość stworzenia listy domen, do których dostęp jest zezwolony(whitelist)/zabroniony(blacklist) niezależnie od konfiguracji filtra URL.
		Administrator musi posiadać możliwość tworzenia listy wyrażeń, których wystąpienie w adresie URL pozwoli na zezwolenie/zablokowanie strony niezależnie od konfiguracji filtra URL.
		Administrator musi posiadać możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z poniższych akcji: • blokowanie dostępu do adresu URL, • zezwolenie na dostęp do adresu URL, • zezwolenie na dostęp do adresu URL po uprzednim wyświetleniu ostrzeżenia.
		Urządzenie musi posiadać wbudowany filtr aplikacji.
		Filtr aplikacji musi zawierać predefiniowane aplikacje i jest dostarczony wraz z urządzaniem (nie wymaga dodatkowej licencji).
		Filtr aplikacji musi wykrywać i umożliwiać blokowanie co najmniej poniższych aplikacji: • komunikatory internetowe: IRC, Pidgin, Jabber, ICQ, Yahoo, MSN, Skype, Gadu-Gadu, GoogleTalk, • odtwarzacze multimedialne: Real Player, iTunes, Spotify, Sopcast, Shoutcase • aplikacje p2p: BitTorrent, Kazaa, • VPN: LogMeIn, TOR, OpenVPN, • VOIP: Netmeeting, Speak Freely, • klienci połączeń terminalowych (RDP): Apple Remote Desktop, LogMeIn, PC Anywhere, VNC.
		Administrator musi posiadać możliwość konfiguracji reguł filtrowania URL i filtra aplikacji mających zastosowanie dla: • zautoryzowanych użytkowników, • niezautoryzowanych użytkowników, • użytkownika/grupy użytkowników z wewnętrznej/zewnętrznej bazy użytkowników, • pojedynczego/grupy adresów IP.

		Reguły filtrowania URL i filtr aplikacji mogą być stosowane cały czas lub według przygotowanego przez administratora harmonogramu określającego dzień tygodnia oraz godzinę działania reguły. Harmonogram ma być konfigurowalny z dokładnością do jednej minuty.
		Urządzenie musi umożliwiać identyfikację oraz blokowanie przesyłanych danych z wykorzystaniem typu MIME.
		Urządzenie musi umożliwiać inspekcję ruchu https tunelowanego wewnątrz protokołu SSL.
		Urządzenie musi umożliwiać skanowanie antywirusowe, antymalware i blokowanie aplikacji wewnątrz protokołu SSL.
		Urządzenie musi umożliwiać włączenie mechanizmu SafeSearch dla wyników wyszukiwania.
		Administrator ma możliwość instalacji Web Security Agent na stacjach z systemem Windows 7/8/10 oraz MAC OS X v10.5 i powyżej.
		Administrator ma możliwość instalacji dodatku Chromebook Security Extension w urządzeniach Chromebook.
		Administrator ma możliwość uruchomienia Safe Browser na urządzeniach mobilnych z iOS 4.3 i powyżej
4.	Administracja	Urządzenie musi być konfigurowane za pomocą graficznego interfejsu dostępnego przez przeglądarkę internetową. Konfiguracja musi być możliwa z użyciem bezpiecznego połączenia poprzez protokół https.
		Interfejs użytkownika musi być dostępny co najmniej w języku polskim i angielskim.
		Urządzenie musi posiadać mechanizm informowania administratora o wystąpieniu problemów za pośrednictwem automatycznie generowanych wiadomości wysyłanych pocztą elektroniczną.
		Urządzenie musi posiadać możliwość eksportowania logów na zewnętrzny serwer (syslog).
		Urządzenie musi posiadać wbudowany w graficzny interfejs administracyjny moduł diagnostyki sieci obejmujący co najmniej następujące polecenia diagnostyczne: ping, telnet, Dig/NS-lookup, TCP dump, traceroute.
5.	Raportowanie	Urządzenie musi posiadać wbudowany mechanizm generowania raportów graficznych.
		Urządzenie musi posiadać możliwość generowania raportów na żądanie (z interfejsu administracyjnego) oraz według zdefiniowanego harmonogramu.
		Urządzenie musi posiadać możliwość generowania raportów według harmonogramu z funkcją wysyłania na zewnętrzny serwer plikowy (SMB lub FTP) lub poprzez automatycznie generowane wiadomości poczty elektronicznej dla jednego lub grupy adresatów.
		Urządzenie musi umożliwiać generowane raportów na żądanie co najmniej w następujących formatach: PDF, html, CSV, txt.
		Urządzenie musi posiadać możliwość uruchomienia usługi Syslog.
		Urządzenie musi zapewniać wsparcie dla SNMP.
9.	Gwarancja i wsparcie techniczne	Gwarancja producenta – 5 lat.
		Automatyczne aktualizacje mechanizmów bezpieczeństwa – 5 lat, m.in.: • Sygnatur wirusów, • Bazy URL, wraz z możliwością odpłatnego przedłużenia licencji po jej wygaśnięciu na kolejny okres minimum jednego roku.
		Aktualizacje oprogramowania – 5 lat.
		Całodobowe wsparcie techniczne (mail/telefon) producenta – 5 lat.
		Dodatkowe wsparcie techniczne (w języku polskim) świadczone przez dystrybutora – 5 lat.
		Wsparcie rozszerzone: w przypadku awarii wysyłka nowego sprzętu następnego dnia roboczego – 5 lat.

		Jeśli w okresie ważności aktywnych serwisów: podstawowego oraz rozszerzonego, zamawiający nie skorzysta z przysługującego mu prawa wymiany zakupionego urządzenia na nowe, to po 4 latach od dnia aktywacji urządzenia Wykonawca zapewni wymianę urządzenia na najnowszy model (odpowiednik posiadanego) bez dodatkowych opłat.
10.	Wykaz oświadczeń i dokumentów, jakie dostarczy Wykonawca w celu potwierdzenia zgodności oferowanych urządzeń z przedmiotem zamówienia	Oświadczenie o posiadaniu deklaracji zgodności CE dla oferowanego urządzenia
		Oświadczenie wskazujące autoryzowany przez producenta urządzenia podmiot do realizowania serwisu gwarancyjnego na terenie Polski oraz że firma serwisująca posiada certyfikat ISO 9001:2000 lub równoważny na świadczenie usług serwisowych
		Oświadczenie Wykonawcy, że posiada autoryzację producenta lub autoryzowanego dystrybutora w zakresie sprzedaży na terenie Polski oferowanego urządzenia oraz świadczenia usług z nim związanych
		Specyfikacja techniczna oferowanego urządzenia
11.	Usługi dodatkowe	Instalacja, wdrożenie i przeszkolenie personelu IT zamawiającego (jednodniowe 8 godzinne warsztaty w siedzibie Zamawiającego – 2 administratorów)

Wykonawca wykona prace instalacyjne i konfiguracyjne polegające na:

1. Instalacji dostarczonego sprzętu w siedzibie Zamawiającego.
2. Zainstaluje i zaktualizuje dostarczone wraz ze sprzętem oprogramowanie (firmware, inne niezbędne do jego prawidłowej konfiguracji) wszystkich urządzeń będących elementami wdrożenia.
3. Konfiguracji urządzenia zgodnie z potrzebami Zamawiającego.
4. Wykonanie dokumentacji powdrożeniowej (w formie pisemnej edytowalnej) zawierającej opis skonfigurowanego serwera proxy.
5. Przeszkolenie przez Wykonawcę w siedzibie Zamawiającego 2 administratorów w zakresie konfiguracji i eksploatacji dostarczonego sprzętu.

Wykonawca zapewni powdrożeniowe wsparcie w siedzibie Zamawiającego w wymiarze do 32h przez okres 12 miesięcy w dni robocze w godzinach 8.00 – 16.00 od daty podpisania protokołu odbioru bez zastrzeżeń, przez osoby realizujące niniejszą Umowę ze Strony Wykonawcy i Zamawiającego.