|  |  |
| --- | --- |
| Parametr | Parametry oferowanego przedmiotu zamówienia  - należy określić rzeczywiste parametry oferowanego przez wykonawcę przedmiotu zamówienia; dopuszcza się wpisanie spełnia / nie spełnia ale zweryfikowanie wskazanego parametru musi być możliwe za pomocą załączonej do oferty karty technicznej produktu lub innego równoważnego dokumentu  - określenie poniższych parametrów nie zwalnia Wykonawcy ze spełnienia zapisów określonych w szczegółowym opisie przedmiotu zamówienia dla danej części. |
| Model urządzenia firewall |  |
| Możliwość pracy urządzenia firewall w następujących trybach: Routera z funkcją NAT oraz trybie transparentnym |  |
| Możliwość utworzenia kont co najmniej 3 administratorów urządzenia firewall |  |
| Wsparcie przez urządzenie firewall protokołów IPv4 oraz IPv6 w zakresie: Firewall, Ochrony w warstwie aplikacji i Protokołów routingu dynamicznego. |  |
| Możliwość połączenia urządzenia firewall pełniącego funkcję Firewall, IPSec, Kontrola Aplikacji i IPS w klaster Active-Active lub Active-Passive. |  |
| Możliwość synchronizacji sesji firewall w urządzeniu firewall |  |
| Możliwość monitoringu i wykrywania uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych w urządzeniu firewall |  |
| Możliwość monitoringu stanu realizowanych połączeń VPN w urządzeniu firewall |  |
| Możliwość agregacji linków przez urządzenie firewall: statycznej oraz w oparciu o protokół LACP |  |
| Ilość i typ portów sieciowych w urządzeniu firewall |  |
| Wyposażenie urządzenia firewall w port konsoli szeregowej |  |
| Wyposażenie urządzenia firewall gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. |  |
| Możliwość zdefiniowania w urządzeniu firewall co najmniej 100 interfejsów wirtualnych definiowanych jako VLAN’y w oparciu o standard 802.1Q. |  |
| Wyposażenie urządzenia firewall w zasilanie AC. |  |
| Ilość jednoczesnych połączeń obsługiwanych przez urządzenie firewall |  |
| Ilość nowych połączeń na sekundę obsługiwanych przez urządzenie firewall |  |
| Przepustowość Stateful Firewall w urządzeniu firewall |  |
| Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji w urządzeniu firewall |  |
| Wydajność szyfrowania IPSec VPN w urządzeniu firewall |  |
| Wydajność skanowania ruchu w celu ochrony przed atakami w urządzeniu firewall (zarówno client side jak i server side w ramach modułu IPS) |  |
| Wydajność urządzenia firewall w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http |  |
| Zapewnienie przez Urządzenie firewall kontroli dostępu (zapora ogniowa klasy Stateful Inspection) |  |
| Zapewnienie przez Urządzenie firewall kontroli Aplikacji |  |
| Zapewnienie przez Urządzenie firewall poufności transmisji danych (połączenia szyfrowane IPSec VPN oraz SSL VPN) |  |
| Zapewnienie przez Urządzenie firewall ochrony przed malware (co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP i HTTPS) |  |
| Zapewnienie przez Urządzenie firewall ochrony przed atakami (Intrusion Prevention System) |  |
| Zapewnienie przez Urządzenie firewall kontroli stron WWW) |  |
| Zapewnienie przez Urządzenie firewall kontroli zawartości poczty – Antyspam dla protokołów SMTP, POP3) |  |
| Zapewnienie przez Urządzenie firewall zarządzania pasmem (QoS, Traffic shaping) |  |
| Zapewnienie przez Urządzenie firewall analizy ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2 |  |
| Zapewnienie przez Urządzenie firewall funkcji lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system |  |
| Uwzględnienie w polityce Firewall urządzenia firewall adresów IP, użytkowników, protokołów, usług sieciowych, aplikacji lub zbiorów aplikacji, reakcji zabezpieczeń, rejestrowania zdarzeń |  |
| Zapewnienie przez urządzenie firewall translacji adresów NAT: źródłowego i docelowego, translacji PAT oraz translacji jeden do jeden oraz jeden do wielu |  |
| Możliwość tworzenia w ramach urządzenia firewall wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN |  |
| Możliwość wykorzystania w polityce bezpieczeństwa urządzenia firewall zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe |  |
| Możliwość konfiguracji połączeń typu IPSec VPN |  |
| Zapewnienie przez urządzenie firewall wsparcia dla IKE v1 oraz v2 w ramach konfiguracji połączeń typu IPSec VPN |  |
| Zapewnienie przez urządzenie firewall obsługi szyfrowania protokołem AES z kluczem 128 i 256 bitów w ramach konfiguracji połączeń typu IPSec VPN |  |
| Zapewnienie przez urządzenie firewall obsługi protokołu Diffie-Hellman grup 19 i 20 w ramach konfiguracji połączeń typu IPSec VPN |  |
| Zapewnienie przez urządzenie firewall wsparcia dla pracy w topologii Hub and Spoke oraz Mesh w ramach konfiguracji połączeń typu IPSec VPN |  |
| Zapewnienie przez urządzenie firewall tworzenia połączeń typu Site-to-Site oraz Client-to-Site w ramach konfiguracji połączeń typu IPSec VPN |  |
| Zapewnienie przez urządzenie firewall monitorowania stanu tuneli VPN i stałego utrzymywania ich aktywności w ramach konfiguracji połączeń typu IPSec VPN |  |
| Zapewnienie przez urządzenie firewall możliwości wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego w ramach konfiguracji połączeń typu IPSec VPN |  |
| Zapewnienie przez urządzenie firewall obsługi mechanizmów IPSec NAT Traversal w ramach konfiguracji połączeń typu IPSec VPN |  |
| Zapewnienie przez urządzenie firewall mechanizmu „Split tunneling” dla połączeń Client-to-Site w ramach konfiguracji połączeń typu IPSec VPN |  |
| Możliwość konfiguracji połączeń typu SSL VPN |  |
| Zapewnienie przez urządzenie firewall pracy w trybie Portal gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki w ramach połączeń typu SSL VPN |  |
| Zapewnienie przez urządzenie firewall pracy w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta w ramach połączeń typu SSL VPN |  |
| Zapewnienie przez producenta urządzenia firewall oprogramowania klienckiego VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN |  |
| Nazwa oprogramowania klienckiego VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN z urządzeniem firewall |  |
| Zapewnienie przez urządzenie firewall obsługi Routingu statycznego |  |
| Zapewnienie przez urządzenie firewall obsługi Policy Based Routingu |  |
| Zapewnienie przez urządzenie firewall obsługi protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP |  |
| Możliwość wykorzystania protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN w urządzeniu firewall |  |
| Możliwość określenie aplikacji jako argumentu dla kierowania ruchu w regułach SD-WAN w urządzeniu firewall |  |
| Możliwość zarządzania pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu w urządzeniu firewall |  |
| Możliwość określania pasma dla poszczególnych aplikacji w urządzeniu firewall |  |
| Możliwość zarządzania pasmem dla wybranych kategorii URL w urządzeniu firewall |  |
| Możliwość skanowania ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) przez silnik antywirusowy urządzenia firewall |  |
| Możliwość skanowania archiwów, w tym co najmniej: zip, rar przez silnik antywirusowy urządzenia firewall |  |
| Możliwość współpracy silnika antywirusowego urządzenia firewall z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze |  |
| Nazwa zaoferowanej platforma typu Sandbox |  |
| Oparcie ochrony IPS w urządzeniu firewall na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych |  |
| Ochrona przed atakami na aplikacje pracujące na niestandardowych portach w urządzeniu firewall |  |
| Ilość wpisów w bazie sygnatur ataków urządzenia firewall |  |
| Sposób aktualizacji wpisów w bazie sygnatur ataków urządzenia firewall |  |
| Możliwość definiowania własnych wyjątków oraz własnych sygnatur w urządzeniu firewall |  |
| Zapewnienie przez urządzenie firewall wykrywania anomalii ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. |  |
| Zapewnienie przez urządzenie firewall mechanizmów ochrony aplikacji WEB’owych przed: CSS, SQL Injecton, Trojanami, Exploitami, BotNETami |  |
| Zapewnienie przez urządzenie firewall możliwości kontrolowania długości nagłówka, ilości parametrów URL i Cookies |  |
| Zapewnienie przez urządzenie firewall możliwości wykrywania i blokowania komunikacji C&C do sieci botnet |  |
| Możliwość kontroli ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP przez urządzenie firewall |  |
| Ilość wpisów w bazie kontroli aplikacji urządzenia firewall |  |
| Sposób aktualizacji wpisów w bazie kontroli aplikacji urządzenia firewall |  |
| Uwzględnienie w bazie kontroli aplikacji urządzenia firewall kategorii aplikacji proxy i P2P |  |
| Możliwość definiowania wyjątków oraz własnych sygnatur przez administratora urządzenia firewall |  |
| Ilość adresów URL w bazie wykorzystywanej przez moduł kontroli WWW urządzenia firewall |  |
| Pogrupowanie bazy wykorzystywanej przez moduł kontroli WWW urządzenia firewall w kategorie tematyczne |  |
| Lista kategorii dostępnych w ramach filtra www urządzenia firewall |  |
| Możliwość nadpisywania kategorii oraz tworzenia wyjątków przez administratora urządzenia firewall (białe/czarne listy dla adresów URL) |  |
| Możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania urządzenia firewall |  |
| Możliwość określenia, dla których kategorii url lub adresów url urządzenie firewall nie będzie dokonywało inspekcji szyfrowanej komunikacji |  |
| Możliwość weryfikacji tożsamości użytkowników urządzenia firewall za pomocą haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu |  |
| Możliwość weryfikacji tożsamości użytkowników urządzenia firewall za pomocą haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP |  |
| Możliwość weryfikacji tożsamości użytkowników urządzenia firewall za pomocą haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych |  |
| Możliwość zastosowania do weryfikacji tożsamości użytkowników procesu uwierzytelniania dwu-składnikowego |  |
| Możliwość budowy w urządzeniu firewall architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory |  |
| Możliwość zarządzania lokalnego urządzeniem firewall z wykorzystaniem protokołów: HTTPS oraz SSH |  |
| Możliwość współpracy urządzenia firewall z dedykowanymi platformami centralnego zarządzania i monitorowania. |  |
| Możliwość komunikacji systemów zabezpieczeń urządzenia firewall z platformami centralnego zarządzania z wykorzystaniem szyfrowanych protokołów |  |
| Współpraca urządzenia firewall z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c i 3 |  |
| Zapewnienie przez producenta zaoferowanego urządzenia firewall wbudowanego narzędzia diagnostycznego posiadającego przynajmniej: ping, traceroute, podgląd pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall |  |
| Możliwość logowania przez urządzenie firewall do centralnego systemu logowania i raportowania posiadanego przez Zamawiającego lub do komercyjnego system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej |  |
| Nazwa komercyjnego system logowania i raportowania zaoferowanego w ramach postepowania w przypadku braku możliwości logowania z urządzenia firewall do centralnego systemu logowania i raportowania posiadanego przez Zamawiającego |  |
| Zapewnienie przez urządzenie firewall przekazywania logów z danymi o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu |  |
| Możliwość jednoczesnego wysyłania przez urządzenie firewall logów do wielu serwerów logowania |  |
| Logowanie przez urządzenie firewall zdarzeń dotyczących wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu |  |
| Możliwość logowania do serwera SYSLOG przez urządzenie firewall |  |
| Certyfikaty posiadane przez zaoferowane urządzenie firewall dla funkcji Firewall |  |
| Certyfikaty posiadane przez zaoferowane urządzenie firewall dla funkcji VPN |  |
| Okres możliwości korzystania z aktualnych baz funkcji ochronnych producenta i serwisów w ramach zaoferowanej do urządzenia firewall licencji dla modułów: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, Bazy reputacyjne adresów IP/domen |  |
| Okres trwania serwisu gwarancyjnego producenta dla urządzenia firewall |  |
| Okres dostępu do aktualizacji oprogramowania oraz wsparcia techniczne w trybie 24x7 dla urządzenia firewall |  |
| Podmiot realizujący pierwszą linię wsparcia technicznego w języku polskim dla urządzenia |  |
| Możliwość wykonania szeregu zmian przez administratora urządzenia firewall w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone |  |
| Zapewnienie przez urządzenie firewall funkcji Safe Search przeciwdziałającej pojawianiu się niechcianych treści w wynikach wyszukiwarek takich jak Google i Yahoo |  |
| Możliwość tworzenia interfejsów redundantnych w urządzeniu firewall |  |
| Możliwość pracy urządzenia firewall w trybie monitorowania na porcie SPAN |  |
| Możliwość budowy w dostarczonym urządzeniu firewall minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji |  |
| Możliwość dedykowania administratorów do poszczególnych instancji systemu w urządzeniu firewall |  |
| Możliwość współpracy zaoferowanego urządzenia firewall z posiadanym przez Zamawiającego systemem logowania i raportowania FortiAnalyzer-VM |  |
| Model Access Pointa |  |
| Możliwość kontrolowania Access Point’ów przez posiadane przez Zamawiającego urządzenia Fortigate 50E |  |
| Możliwość kontrolowania Access Pointów przez zaoferowane przez w ramach postepowania urządzenie firewall |  |
| Ilość zaoferowanych kontrolerów sprzętowych dla Access Pointów w przypadku zaoferowania alternatywnych kontrolerów sprzętowych |  |
| Model zaoferowanych kontrolerów sprzętowych dla Access Pointów w przypadku zaoferowania alternatywnych kontrolerów sprzętowych |  |
| Możliwości montażu Access Pointa zapewnione przez obudowę urządzenia |  |
| Temperatura w jakiej producent Access Pointów zapewnia prawidłową pracę urządzenia |  |
| Wilgotność w jakiej producent Access Pointów zapewnia prawidłową pracę urządzenia |  |
| Ilość niezależnych modułów radiowych Access Pointów |  |
| Pasma w których pracują modiły radiowe Access Pointów |  |
| Standardy jakie obsługują moduły radiowe Access Pointów |  |
| Ilość SSID które Access Pointy mogą rozgłaszać jednocześnie |  |
| Ilość interfejsów Ethernet w które są wyposażone Access Pointy |  |
| Standard interfejsów Ethernet w które są wyposażone Access Pointy |  |
| Sposób zasilania Access Pointów |  |
| Tryby przesyłania danych umożliwione przez Access Pointy |  |
| Wsparcie przez Access Pointy dla QoS |  |
| Możliwość konfigurowania polityk QoS Access Pointów per użytkownik/aplikacja |  |
| Metod uwierzytelnienia dla których wsparcie zapewniają Access Pointy |  |
| Wsparcie interfejsu radiowego Access Pointów dla funkcji MIMO – 2x2 |  |
| Maksymalna przepustowość dla poszczególnych modułów radiowych Access Pointów |  |
| Moc nadawania dla poszczególnych pasm radiowych obsługiwanych przez Access Pointy |  |
| Możliwość wyłączenia nieużywanego moduł radiowego w celu obniżenia poboru mocy |  |
| Maksymalna liczba klientów per moduł radiowy Access Pointa |  |
| Certyfikaty posiadane przez zaoferowane Access Pointy |  |
| Zapewnienie przez producenta zaoferowanych Access Pointów ograniczonej gwarancji producenta do 5 lat od zaprzestania produkcji |  |
| Okres trwania serwisu gwarancyjnego producenta dla Access  Pointów |  |
| Okres dostępu do aktualizacji oprogramowania oraz wsparcia techniczne w trybie 24x7 dla urządzenia firewall |  |
| Podmiot realizujący pierwszą linię wsparcia technicznego w języku polskim dla urządzenia |  |
| Nazwa licencji serwisowej zaoferowanej dla routera Fortigate-61F lub rozwiązania alternatywnego |  |
| Lista modułów objętych wsparciem w ramach zaoferowanej licencji dla routera Fortigate-61F lub rozwiązania alternatywnego |  |
| Okres trwania wsparcia technicznego w ramach zaoferowanej licencji dla routera Fortigate-61F lub rozwiązania alternatywnego |  |
| Godziny oraz dni w jakich dostępne będzie wsparcie w ramach zaoferowanej licencji dla routera Fortigate-61F lub rozwiązania alternatywnego |  |
| Nazwa licencji serwisowej zaoferowanej dla routera FortiGate-50E lub rozwiązania alternatywnego |  |
| Ilość licencji serwisowych zaoferowanych dla routera FortiGate-50E lub ilość rozwiązań alternatywnych |  |
| Lista modułów objętych wsparciem w ramach zaoferowanej licencji dla routera Fortigate-50E lub rozwiązania alternatywnego |  |
| Okres trwania wsparcia technicznego w ramach zaoferowanej licencji dla routera Fortigate-50E lub rozwiązania alternatywnego |  |
| Godziny oraz dni w jakich dostępne będzie wsparcie w ramach zaoferowanej licencji dla routera Fortigate-50E lub rozwiązania alternatywnego |  |
| Nazwa licencji FortiAnalyzer-VM |  |
| Okres trwania licencji FortiAnalyzer-VM |  |
| Godziny oraz dni w jakich dostępne będzie wsparcie w ramach zaoferowanej licencji dla routera Fortigate-50E lub rozwiązania alternatywnego |  |
| Ilość danych jakie mogą zostać dziennie przesłane w ramach zaoferowanej licencji FortiAnalyzer-VM |  |

**Lista dokumentów które muszą zostać załączone do formularza oferty**

(dokumenty muszą być wystawione w języku polskim lub angielskim)

1. Karta produktowa umożliwiającą weryfikację wymaganych parametrów oferowanego sprzętu lub inny równoważny dokument
2. Certyfikat ICSA lub EAL4 dla funkcji Firewall oferowanego urządzenia firewall
3. Certyfikat ICSA lub EAL4 dla funkcji VPN oferowanego urządzenia firewall
4. Certyfikat ISO 9001 w zakresie świadczenia usług serwisowych dla urządzenia firewall wystawiony dla Wykonawcy lub Autoryzowanego Dystrybutora
5. Oświadczanie Autoryzowanego Dystrybutora świadczącego wsparcie techniczne dla urządzenia firewall o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu w przypadku gdy Wykonawca nie będzie świadczył wsparcia technicznego dla oferowanego urządzenia
6. Oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanego urządzenia firewall
7. Certyfikat ISO 9001 w zakresie świadczenia usług serwisowych dla Access Pointów wystawiony dla Wykonawcy lub Autoryzowanego Dystrybutora
8. Oświadczanie Autoryzowanego Dystrybutora świadczącego wsparcie techniczne dla Access Pointów o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu w przypadku gdy Wykonawca nie będzie świadczył wsparcia technicznego dla oferowanego urządzenia
9. Oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych Access Pointów