*Załącznik nr 1 do zapytania ofertowego*

**FORMULARZ OFERTOWY**

|  |  |
| --- | --- |
| ***Przedmiot zamówienia*** | **„FORTIGATE 300C „** |
| ***Zamawiający*** | ***Szpital Specjalistyczny w Pile im. Stanisława Staszica******64–920 Piła, ul. Rydygiera 1*** |
| ***Oferent – pełna nazwa Oferenta,******adres,******tel., fax.******NIP******REGON******e-mail*** |  |
| ***Oferowana wartość******za wykonanie******zadanie****(podlega ocenie)* | **wartość netto:……………………………….****słownie: ………………………………………………………………..****stawka VAT: ………………………..****wartość brutto: ……………………………………………….** |
| ***Termin płatności*** | **60 dni** |
| ***Termin realizacji zamówienia*** | **20.02.2020** |
| ***Imiona, Nazwiska, osób upoważnionych do podpisania umowy******(zgodnie z ustanowioną zasadą reprezentacji)*** |  |
| **ZOBOWIĄZANIA W PRZYPADKU PRZYZNANIA ZAMÓWIENIA:**1. zobowiązujemy się do zawarcia umowy w miejscu i terminie wyznaczonym przez Zamawiającego;
2. osoby które będą zawierały umowę ze strony Wykonawcy:

.......................................................................................................................................................................e-mail:………...……........……………………………..……....….tel....................................................………………..;1. osobą odpowiedzialną za realizację umowy jest:

.......................................................................................................................................................................e-mail:………...……........……………………………..……....….tel....................................................………………..; |

*oświadczam, że:*

*Oświadczamy, że zapoznaliśmy się z opisem przedmiotu zamówienia i nie wnosimy do niego żadnych uwag oraz uzyskaliśmy konieczne informacje i wyjaśnienia niezbędne do przygotowania oferty.*

*Oświadczamy, że czujemy się związani ofertą na czas wskazany w zapytaniu ofertowym istotnych warunków zamówienia, tj. przez okres 30 dni, licząc od upływu składania ofert.*

*Oświadczamy, że zapoznaliśmy się z projektem umowy i nie wnosimy zastrzeżeń, co do jej treści.*

*Oświadczamy, że zapoznaliśmy się z informacją RODO i Instrukcją bezpieczeństwa i higieny prac realizowanych przez podmioty zewnętrzne na terenie Szpitala Specjalistycznego w Pile im. Stanisława Staszica .*

*Oświadczamy, że cena brutto podana w niniejszym formularzu zawiera wszystkie koszty wykonania zamówienia, jakie ponosi Zamawiający w przypadku wyboru niniejszej oferty.*

*Oświadczamy, iż powyższe zamówienie w całości zrealizujemy sami.*

Załącznikami do niniejszej oferty są:

1. ………………………………………………………………………………………………………………….
2. ………………………………………………………………………………………………………………….
3. ………………………………………………………………………………………………………………….
4. ………………………………………………………………………………………………………………….
5. ………………………………………………………………………………………………………………….
6. ………………………………………………………………………………………………………………….

Oferta została złożona na ....... zapisanych i kolejno ponumerowanych oraz podpisanych stronach.

 dnia …………………………………………………………….

podpis osoby uprawnionej do składania oświadczeń woli w imieniu Wykonawcy

Załącznik nr 2 do zapytania ofertowego

Przedmiotem zamówienia jest zakup oraz wymiana sprzętu zapory sieciowej tzw. Firewall wraz z oprogramowaniem dla Szpitala Specjalistycznego w Pile im. Stanisława Staszica

**Szczegółowy opis przedmiotu zamówienia**

Przedmiotem zamówienia jest wymiana urządzeń firmy Fortinet wchodzących w skład infrastruktury sieciowej i bezpieczeństwa Zamawiającego tj.w Szpitalu Specjalistycznym w Pile im.Stanisława Staszica 64-920 Piła ul. Rydygiera 1 wraz z usługą wymiany i przeniesienia konfiguracji z urządzeń podlegających wymianie.

Zamawiający posiada następujące urządzenia podlegające wymianie: FortiGate 300C – 2 szt.

Szczegółowe dane urządzeń:

|  |  |  |
| --- | --- | --- |
| **Producent** | **Model** | **Numer Seryjny** |
| Fortinet | FortiGate300C | FG300C3912603086 |
| Fortinet | FortiGate300C | FG300C3913605610 |

Zamawiający posiada również 60 szt. bezprzewodowych punktów dostępowych FAP-221C, dla których klaster HA FortiGate 300C pełni funkcję kontrolera bezprzewodowego. Po wymianie urządzeń na nowe funkcjonalność ta musi zostać zachowana.

Powyższe urządzenia użytkowan esą w siedzibie Zamawiającego. Dostarczone urządzenia muszą zostać w pełni skonfigurowane na miejscu w siedzibie Zamawiającego przez osoby wyznaczone przez Wykonawcę do realizacji zamówienia.

Po wymianie, urządzenia muszą spełniać następujące minimalne parametry techniczne:

**Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSecVPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.

System musi wspierać 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 – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:
* 18 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 4 mln jednoczesnych połączeń oraz 300.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 32 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 7 Gbps.
4. Wydajność szyfrowania IPSec VPN: nie mniej niż 15 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3.9 Gbps.

**Funkcje Systemu Bezpieczeństwa:**

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

1. Kontrola dostępu - zapora ogniowa klasy StatefulInspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami -IntrusionPrevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Trafficshaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone 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. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

**Polityki, Firewall**

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dlaprotokołu SIP.
1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

**Połączenia VPN**

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
* Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/CounterMode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19 i 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
* 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.
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.
1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

**Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
* Routingu statycznego.
* Policy Based Routingu.
* Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
1. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

**Zarządzanie pasmem**

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

**Kontrola Antywirusowa**

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

**Ochrona przed atakami**

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać 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) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

**Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

**Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

**Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać 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.
1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

**Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

**Logowanie**

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
3. Musi istnieć możliwość logowania do serwera SYSLOG.

**Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.
* ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.
* ICSA dla funkcji SSL VPN.

**Serwisy i licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a)     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 na okres 12 miesięcy.

**Gwarancja oraz wsparcie**

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.
2. **Opisy do wymagań ogólnych:**
3. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
4. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.