Opis zakresu szacowania ceny

„Modernizacja urządzeń brzegowych”

I. Nazwa Zamówienia:

Modernizacja urządzeń brzegowych

II. Przedmiot zamówienia:

Modernizacja urządzeń brzegowych, w której skład wchodzą:

a) dostawa przedmiotu zamówienia do siedziby Zamawiającego,

b) wdrożenie wraz z konfiguracją,

c) wsparcie powdrożeniowe.

III. Kody CPV:

48000000-8 Pakiety oprogramowania i systemy informatyczne.

32420000-3 Urządzenia sieciowe.

35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa.

72250000-2 Usługi w zakresie konserwacji i wsparcia systemów.

IV. Czas realizacji zamówienia:

- 60 dni

V. Wymagania ogólne:

Zamawiający wymaga, by dostarczone rozwiązanie było nowe oraz nieużywane.

Wykonawca powinien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż posiada autoryzację producenta na terenie Polski w zakresie sprzedaży oferowanych rozwiązań.

Rozwiązanie musi być objęte serwisem gwarancyjnym producenta 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 24x7.

Wykonawca musi dostarczyć wszystkie niezbędne platformy oraz licencje umożliwiające i upoważniające do korzystania z aktualnych baz i serwisów producenta dla funkcji zaoferowanego rozwiązania.

Minimalne wymagania:

Zapora Sieciowa (Firewall) – 2 szt.

Musi zapewniać wszystkie wymienione poniżej funkcje sieciowe oraz bezpieczeństwa, niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w jej skład były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z systemem operacyjnym.

Zaoferowane rozwiązanie powinno posiadać certyfikacje ICSA lub EAL4.

W ramach postępowania zapora sieciowa musi zostać dostarczona w postaci klastra urządzeń.

Zapora Sieciowa (Firewall) musi mieć możliwość pracy w jednym z trzech trybów:

- routera z funkcją NAT,
- transparentnym,
- 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, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

Powinna posiadać możliwość ustanowienia co najmniej 4 administratorów do poszczególnych instancji systemu.

Musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall,
- ochrony w warstwie aplikacji,
- protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii:

1. W przypadku zapory sieciowej pełniącej 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. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Musi istnieć możliwość tworzenia interfejsów redundantnych.

Parametry fizyczne:

1. Interfejsy/porty:
   - 18 portów Gigabit Ethernet RJ-45,
   - 8 portów SFP 1 Gbps,
   - 4 porty SFP+ 10 Gbps,

- możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych (VLAN) w oparciu o standard 802.1Q.

2. Wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu (3G/4G) oraz instalacji oprogramowania (np. poprzez klucz USB).
3. Montaż w szafie RACK.
4. Posiada redundantne zasilacze AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 260 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 26 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 13 Gbps.
4. Wydajność szyfrowania IPSec VPN: nie mniej niż 12 Gbps.
5. Ilość jednoczesnych połączeń SSL VPN : nie mniej niż 300.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (po stronie klienta jak i serwera w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps.

Realizowane Funkcje:

W ramach oferowanego rozwiązania muszą być realizowane wszystkie poniższe funkcje. Zamawiający dopuszcza aby były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Kontrola stron WWW.
4. Ochrona przed atakami - Intrusion Prevention System.
5. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
6. Poufność transmisji danych – połączenia szyfrowane IPSec VPN oraz SSL VPN.
7. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony DLP.
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 takie 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, także dla protokołu HTTP/2,
    - SSH.
12. Funkcja 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.

Zarządzanie Politykami bezpieczeństwa:

1. Polityki Firewall muszą uwzględniać obiekty typu: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub grupy aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. Powinna również istnieć możliwość łączenia w grupy ww. obiektów np. grupa użytkowników, protokołów.
2. Musi być zapewniona translacja adresów:
    - NAT - źródłowego i docelowego,
    - translację PAT,
    - translację jeden do jeden oraz jeden do wielu,
    - dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. Musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających:
    - kategorie url,
    - adresy IP,
    - nazwy domenowe,
    - hash'e złośliwych plików.
5. Możliwość integracji z rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych aby użyć ich przy budowaniu polityk kontroli dostępu dla co najmniej:
    - VMware NSX,
    - Microsoft Azure,
    - Google Cloud Platform (GCP),
    - Amazon Web Services (AWS).

Połączenia typu VPN:

1. Musi być zapewniona możliwość konfiguracji połączeń typu IPSec VPN w zakresie:
    - wsparcie dla IKE v1 oraz v2,
    - obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(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 połączeń VPN i stałego utrzymywania ich aktywności,
    - możliwość wyboru tunelu przez protokoły routingu dynamicznego lub statycznego,
    - obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth,
    - mechanizm dzielonego tunelowania dla połączeń klienckich.
    - obsługa minimum 300 jednoczesnych połączeń vpn client to side
2. 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 dzielonego tunelowania przy zastosowaniu dedykowanego klienta.

- producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń typu:
    - IPSec VPN lub SSL VPN.

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.

Funkcje SD-WAN

1. Możliwość wykorzystania protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. Zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. Możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Możliwość skanowania ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
2. Możliwość skanowania archiwów co najmniej: zip, RAR.
3. Zapora musi dysponować sygnaturami do ochrony urządzeń mobilnych co najmniej dla systemu operacyjnego Android.
4. Realizacja współpracy z dedykowaną platformą lub usługą typu Sandbox lokalnie lub w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI rozwijanego przez producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Ochrona przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać co najmniej 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. 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. 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 2000 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. Możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Kontrola 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, lub inne będące źródłem złośliwego oprogramowania
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. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia wyłączeń, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników

1. Możliwość weryfikacji tożsamości użytkowników za pomocą haseł statycznych lub dynamicznych i definicji użytkowników:
    - przechowywanych w lokalnej bazie systemu,
    - bazach zgodnych z LDAP,
    - w oparciu o zewnętrzne bazy danych (RADIUS, RSA SecurID),
    - możliwość zastosowania w tym procesie uwierzytelniania dwu składnikowego.
2. Możliwość wykorzystania uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów typu RADIUS lub API.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinna istnieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania:
    - komunikacja z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
2. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

3. Współpraca z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
4. Możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
5. Wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podgląd pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
6. Możliwość dokonania zmian poprzez CLI lub GUI dl funkcji, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Logowanie do komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej. System logowania realizujący te funkcje jest również przedmiotem postępowania.
2. W ramach logowania zapora sieciowa musi zapewniać przekazywanie danych o ruchu zaakceptowanym/blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego rozwiązania.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Urządzenie typu AccesPoint – 6 szt.

Urządzenie ma realizować funkcje punktu dostępowego zarządzanego z poziomu kontrolera sieci bezprzewodowej. Kontrolerem tym powinny być urządzenia firewall będące przedmiotem postępowania. Jeżeli zaoferowane rozwiązanie firewall nie realizuje takiej funkcji należy dostarczyć dodatkowo dwa redundantne kontrolery sprzętowe obsługujące co najmniej 128 urządzeń AP wraz z gwarancją.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
    - temperatura 0–45°C,
    - wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington.
3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
    - 2.4 GHz 802.11b/g/n,
    - 5 GHz 802.11a/n/ac/ax,
    - Skaner 2.4GHz i 5GHz.
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej:
    - 16 SSID.
5. Urządzenie musi być wyposażone w dwa interfejsy Ethernet:
    - 10/100/1000 Base-TX,
    - 10/100/1000/2500 Base-TX.

6. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz.
7. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
    - Tunnel,
    - Bridge,
    - Mesh.
8. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS na użytkownika lub aplikację.
9. Wsparcie dla poniższych metod uwierzytelnienia:
    - WEP,
    - WPA-PSK, WPA-TKIP,
    - WPA2-AES,
    - Web Captive Portal,
    - MAC blacklist & whitelist,
    - 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
10. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    - MIMO – 4x4.
11. Maksymalna przepustowość dla poszczególnych modułów radiowych:
    - 1147 Mbps,
    - 2402 Mbps.
12. Wymagana moc nadawania:
    - min. 23 dBm dla pasma 2.4GHz, 5GHz,
    - możliwość zmiany mocy co 1dBm.
13. Wsparcie dla:
    - 802.11n 20/40Mhz HT,
    - kanałów 80 i 160 MHz.
14. Anteny:
    - 5 zewnętrznych dla nadajników standardu 802.11 o zysku min.:
        - 4dBi dla pasma 2.4GHz,
        - 6dBi dla pasma 5GHz.
15. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
16. Maksymalna deklarowana liczba klientów per moduł radiowy:
    - 512.
17. Funkcje dodatkowe:
    - MIMO Power Save,
    - Low-Density Parity Check (LDPC) Encoding,
    - Maximum Likelihood Demodulation (MLD),
    - Maximum Ratio Combining (MRC),
    - A-MPDU and A-MSDU Packet Aggregation,
    - Short Guard Interval.

System Logowania/Analizy ruchu sieciowego – 1 szt.

Oferowane rozwiązanie musi współpracować i być kompatybilne z oferowaną zaporą sieciową umożliwiając odbiór, analizę oraz przechowywanie zbieranych zdarzeń oraz być zgodne z:

Parametry fizyczne:

- wyposażony w minimum 2 porty Gigabit Ethernet RJ-45,
- zasoby dyskowe co najmniej 4 TB,
- zasilacz AC.

Parametry wydajnościowe:

- odbiór minimum 100 GB zdarzeń dziennie,
- analiza od 3000 logów na sekundę,
- kolekcjonowanie logów z co najmniej 20 systemów.

Logowanie

- podgląd zdarzeń w czasie rzeczywistym,
- możliwość przeglądania i filtrowania logów historycznych,
- wbudowane lub edytowalne raporty graficzne lub tekstowe wizualizujące stan pracy urządzenia oraz informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej listy oraz informacje:
    - najczęściej wykrywanych ataków,
    - najczęściej wykorzystywanych aplikacji,
    - najczęściej odwiedzanych stron www,
    - najbardziej aktywnych użytkowników,
    - krajów , do których nawiązywane są połączenia,
    - najczęściej wykorzystywanych polityk Firewall,
    - o realizowanych połączeniach IPSec.
- możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
- komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.

System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

- generowanie raportów co najmniej w formatach: PDF, CSV,
- predefiniowane lub edytowalne zestawy raportów, dla których można modyfikować parametry prezentowania wyników,
- funkcję definiowania własnych raportów.,
- możliwość spolszczenia raportów jeżeli zaoferowane rozwiązanie nie jest polskojęzyczne,
- generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

- korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany,
- konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa,
- wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne w tym co najmniej:

    - malware,
    - aplikacje sieciowe,
    - email,
    - IPS,
    - ruch sieciowy,
    - systemowe tj. utracone połączenie: VPN, sieciowe.

Zarządzanie

- System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów:
    - HTTPS,
    - SSH,
    - lub producent rozwiązania musi dostarczać dedykowaną konsoli zarządzania, która komunikuje się z rozwiązaniem wykorzystując szyfrowane protokoły.
- Proces uwierzytelniania administratorów musi być realizowany w oparciu o:
    - lokalną bazę,
    - Radius,
    - LDAP,
    - PKI.
- System musi umożliwiać utworzenie co najmniej 3 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których dostarczane są zdarzenia.

Dodatkowo

Rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w **Następnym Dniu Roboczym** od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora.

Oferent winien przedłożyć oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu.

Wdrożenie

W ramach postępowania wymaga jest aby zaoferowane rozwiązanie zostało wdrożone w siedzibie Zamawiającego. Tym samym zwiększając poziom bezpieczeństwa i usprawniając procesy zarządzania.

Zamawiający wymaga również aby proces wdrożeniowy odbywał się z w sposób niewpływający na dostępność pozostałych usług lub wpływ ten był ograniczony do minimum, tym samym umożliwiając Zamawiającemu dostosowanie reszty powiązanych zasobów oraz poinstruowanie pracowników w przypadku konieczności zastosowania innego oprogramowania do połączeń VPN niż wykorzystuje.

Aktualna infrastruktura Zamawiającego, która ma zostać zmodernizowana dostarczonym rozwiązaniem składa się z:

- zapory sieciowej
    - SonicWall TZ600 (HA)
- bramki WWW
    - Barracuda Web Security Gateway 300
- bramki VPN
    - SonicWall Mobile Acces 400
- bramki e-mail
    - Barracuda Email Security Gateway 400
- systemu sieci bezprzewodowej
    - Ubiquiti unifi

Urządzenia te podłączone są bezpośrednio do Klastra przełączników szkieletowych:

- Extreme Networks X620-16x-Base

W ramach wdrożenia Wykonawca wykona prace w zakresie:

- dostawy rozwiązania wraz z niezbędnymi serwisami oraz oprogramowaniem.
- instalacji oraz konfiguracji rozwiązania w serwerowni Zamawiającego.
- migracji zasobów/konfiguracji jeżeli będzie wymagana.
- wykonania dokumentacji powdrożeniowej dla dostarczonego rozwiązania w tym z wykonanych prac.
- instruktażu Administratorów Zamawiającego dotyczącego implementowanego rozwiązania w zakresie wdrożenia.
- integracji dostarczonego rozwiązania z pozostałymi zasobami Zamawiającego, np. Active Directory.

Gwarancja oraz wsparcie powdrożeniowe

W trakcie trwania okresu gwarancyjnego wykonawca musi zapewnić pierwszą linię wsparcia:

- w języku polskim,
- w dni robocze w godzinach 8:00 – 16:00.
- wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych.

Od momentu realizacji całości zamówienia potwierdzonej protokołem, Wykonawca na świadczyć na rzecz Zamawiającego powdrożeniowe wsparcie techniczne do oferowanego rozwiązania przez okres 12 miesięcy. W tym celu wykonawca musi posiadać co najmniej dwóch inżynierów posiadających aktualny certyfikat techniczny lub certyfikaty wystawione przez producenta oferowanego rozwiązania potwierdzające wiedzę i obsługę z ich zakresu.

W ramach wsparcia powdrożeniowego Wykonawca na prośbę Zamawiającego będzie dokonywał prac dotyczących dostarczonego rozwiązania w zakresie:

- konfiguracji,
- rozwiązywania problemów dotyczących funkcjonowania,
- wsparcia Zamawiającego w zakresie konfiguracji i obsługi,
- udzielania konsultacji dotyczących:
  - konfiguracji,
  - obsługi,
  - funkcji.

Wsparcie te będzie realizowane:

- w dni robocze w godzinach 8:00 – 16:00
- poprzez zgłoszenie:
  - email, telefoniczne, portal www (jeżeli wykonawca taki posiada)

Czasy reakcji i realizacji:

Czasy reakcji i realizacji zgłoszeń		
Priorytet	**Opis**	**Czas**
Czas Reakcji	Czas reakcji na zgłoszenie	30 minut
Niski	Konsultacje lub problem nie mający wpływu na sieć Zamawiającego	24 godziny
Średni	Problem powodujący dysfunkcję nie mającą wpływu na sieć zamawiającego	12 h
Wysoki	Problem powodujący dysfunkcję utrudniającą pracę sieci zamawiającego	3 h
Krytyczny	Problem powodujący dysfunkcję powodującą utratę lub zastój w pracy sieci zamawiającego	1 h

Zamawiający zapewni dostęp zdalny dla Wykonawcy w celu dokonywania prac serwisowych.