WZP.271.2.2023.E

Załącznik do swz

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa urządzeń typu firewall wraz z licencjami oraz dostawa licencji na urządzenia FortiWeb, FortiMail i FortiAnalyzer w ramach II etapu projektu Platforma Miejska - doposażenie partnerów w sprzęt do wykorzystania w ramach Platformy Miejskiej realizowanego w ramach projektu: „Infostrada Kujaw i Pomorza 2.0" dofinansowanego z Unii Europejskiej w ramach środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020, Oś priorytetowa 2. Cyfrowy region, Działanie 2.1. Wysoka dostępność i jakość e-usług publicznych.

Pakiet I

Przedmiotem zamówienia jest dostawa, instalacja i uruchomienie 2 urządzeń typu firewall następnej generacji (ang. Next-Generation Firewall (NGFW)) w konfiguracji wysokiej dostępności (ang. High Availability – HA)

1. Zamawiający wymaga dostarczenia, instalacji, skonfigurowania i uruchomienia do pracy w Urzędzie Miasta Bydgoszczy **dwóch urządzeń NGFW** - pracujących jako klaster w trybie Active-Active.
2. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane wyłącznie w postaci zamkniętej platformy sprzętowej.
3. W ramach konfiguracji i uruchomienia urządzeń należy przenieść konfigurację z obecnie używanych 2 Fortigate 3000D na nowe urządzenia ew. ją modyfikując w zależności od potrzeb. Instalacja i konfiguracja systemu musi być przeprowadzona przez uprawnioną osobę posiadającą aktualny najwyższy certyfikat producenta w zakresie instalacji i konfiguracji urządzeń objętych niniejszym postępowaniem.
4. Wykonawca przeprowadzi szkolenia w zakresie konfiguracji i obsługi urządzeń dla 3 osób. Minimalny czas szkolenia 30 godzin zajęć. Minimalny zakres szkolenia:
   1) logowanie i monitoring,
   2) konfiguracja polityk firewalla,
   3) lokalne uwierzytelnianie użytkowników,
   4) SSL VPN,
   5) IPSec-VPN,
   6) skanowanie antywirusowe,
   7) filtr stron WWW,
   8) kontrola aplikacji,
   9) konfiguracja Routingu w tym BGP i OSPF,

10) transparentny tryb pracy,
11) wysoka dostępność (Klaster HA - High Availability),
12) Intrusion Prevention System – IPS,
13) Single Sign-On,
14) operacje oparte na certyfikatach,
15) diagnostyka i rozwiązywanie problemów,
16) zasoby systemowe – optymalizacja,
17) rozwiązywanie problemów sieciowych,
18) rozwiązywanie problemów: z uwierzytelnianiem użytkowników, VPN

5. **Wymagania dla urządzenia NGFW.** Urządzenie musi spełniać minimum poniższe wymagania (parametry podane są dla pojedynczego urządzenia):
   1) możliwość łączenia w klaster Active-Active oraz Active-Passive minimum 2 urządzeń,
   2) urządzenia powinny być wyposażone w redundantne zasilacze AC 230V,
   3) monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych,
   4) monitoring stanu realizowanych połączeń VPN,
   5) umożliwiać pracę w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
   6) inspekcja bezpieczeństwa realizowana w trybie: flow, proxy oraz explicit proxy dla ruchu http/https.
   7) posiadać minimum: 2 porty Ethernet 10 Gbps (SFP+), 10 portów Ethernet 10/25G (QSFP28) oraz 4 porty 40Gbps
   8) parametry wydajnościowe urządzenia:
      a) w zakresie Firewall'a obsługa nie mniej niż 12 milionów jednoczesnych połączeń oraz 750 tys. nowych połączeń na sekundę,
      b) przepustowość Statefull Firewall'a: nie mniej niż 190 Gbps (ramki 1518 bajt UDP),
      c) wydajność szyfrowania VPN IPSec: nie mniej niż 50 Gbps,
      d) liczba tuneli IPSec client to Gateway – min. 100 000,
      e) wydajność szyfrowania SSL-VPN: nie mniej niż 11 Gbps,
      f) liczba tuneli SSL-VPN client to Gateway – min. 10 000,
      g) wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 22 Gbps,
      h) wydajność skanowania ruchu z włączonymi funkcjami: IPS, Antivirus i Kontrola Aplikacji (NGFW) min. 17 Gbps,
      i) wydajność skanowania ruchu SSL dla ruchu http – (min. 12 Gbps, liczba jednoczesnych sesji 1 300 000),
      j) opóźnienie firewall max 3,5 µs (64bajty, UDP),
   9) możliwość tworzenia min 1000 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q,
   10) możliwość dodania min. 256 secondary IP na interfejsie,
   11) urządzenie powinno być wyposażone w lokalny dysk SSD o pojemności minimum 1TB do celów logowania i raportowania,
   12) w ramach dostarczonego urządzenia muszą być realizowane wszystkie z poniższych funkcjonalności.:
      a) kontrola dostępu - zapora ogniowa (Firewall) klasy Statefull Inspection,

Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektu.

b) ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS),
c) poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN,
d) ochrona przed atakami - Intrusion Prevention System [IPS],
e) kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących, udostępniających treści typu SPAM, oraz pornografię,
f) kontrola pasma oraz ruchu [QoS, Traffic shaping] co najmniej określanie maksymalnej i gwarantowanej ilości pasma,
g) kontrola aplikacji oraz rozpoznawanie ruchu P2P,
h) możliwość analizy ruchu szyfrowanego protokołem SSL
i) ochrona przed wyciekiem poufnej informacji (DLP)
j) dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych, stosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

13) w zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
a) tworzenie połączeń w topologii Site-to-site oraz Client-to-site,
b) monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności,
c) praca w topologii Hub, Spoke oraz Mesh,
d) możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF,
e) obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
14) obsługa Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły:, OSPF, BGP. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN,
15) translacja adresów NAT adresu źródłowego i NAT adresu docelowego, translację PAT oraz:
    a) Translację jeden do jeden oraz jeden do wielu,
    b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP,
16) polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety),
17) możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ,
18) silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021),
19) ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
20) funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP,
21) baza filtra WWW powinna zawierać adresy URL pogrupowane w kategorie tematyczne. W ramach filtra www powinny być dostępne przynajmniej takie kategorie stron jak: spyware/malware, proxy, adult content, web-based email lub równoważne.

Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektu.

Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.

22) filtr www musi posiadać funkcję Safe Search – przeciwdziałającą pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
23) możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna,
24) automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL,
25) system zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
    a) haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu,
    b) haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP,
    c) haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych,
    d) rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory,
    e) dwuskładnikowego uwierzytelniania z wykorzystaniem tokenów sprzętowych lub programowych, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site (),
26) system powinien mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów,
27) interfejs zarządzający systemu powinien umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone,
28) system musi posiadać certyfikacje ICSA lub EAL4 dla funkcji Firewall,
29) wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

6. **Warunki gwarancji**

1) System firewall powinien być objęty serwisem gwarancyjnym producenta przez okres 4 lat, polegającym na naprawie lub wymianie urządzeń w przypadku ich wadliwości. W okresie gwarancji wymagane jest bezpłatne usuwanie awarii oraz bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii.
2) W okresie gwarancji zamawiający musi mieć dostęp u producenta do wszystkich nowszych wersji dostarczonego oprogramowania (firmware oraz aktualizacje sygnatur dla wszystkich wymaganych funkcjonalności),
3) System musi być objęty gwarancją polegającym na udostępnieniu oraz dostarczeniu sprzętu zastępczego na czas naprawy w trybie (kryterium oceny ofert):

a) 8x5xNBD - dostawa urządzenia zastępczego w następnym dniu roboczym licząc od momentu zaakceptowania zgłoszenia serwisowego (pod warunkiem zgłoszenia serwisowego do godz. 15)
b) 8x5x5BD - dostawa urządzenia zastępczego w ciągu 5 dni roboczych licząc od momentu zaakceptowania zgłoszenia serwisowego (pod warunkiem zgłoszenia serwisowego do godz. 15)

4) Gwarancja musi być realizowana przez producenta rozwiązania lub autoryzowanego dystrybutora. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina - reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym
5) Wymagania powinny być potwierdzone dokumentami:
   a) Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego gwarancję o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).

7. **<u>Wdrożenie</u>**

Konfiguracja dostarczonego sprzętu i oprogramowania (w związku ze specyfiką wdrożenia, prace maja być realizowane przez osobę z certyfikatem o najwyższym poziomie certyfikacji w programie producenta):

a) stworzenie klastra urządzeń,
b) rejestracja urządzeń/wsparcia w systemie producenta,
c) migracja ustawień systemowych z istniejących urządzeń wraz z optymalizacją ustawień,
d) migracja konfiguracji sieciowej z istniejących urządzeń uwzględniająca konieczność zmiany interfejsów,
e) migracja polityk zezwalających na ruch pomiędzy segmentami z istniejących urządzeń wraz z optymalizacją pod kątem bezpieczeństwa,
f) aktualizacja do najnowszej zalecanej wersji oprogramowania,
g) przełączenie sieci na nowy klaster urządzeń,
h) wykonanie testów poprawności pracy klastra,
i) podłączenie klastra do systemu zbierania logów posiadanego przez Zamawiającego,
j) wsparcie techniczne przez okres min. 3 miesięcy polegające na rozwiązywaniu problemów konfiguracyjnych pojawiających się po wdrożeniu nowych urządzeń. Czas reakcji jest nie dłuższy niż 1 godzina - reakcja w postaci połączenia telefonicznego i przystąpienia do rozwiązywania problemu przez specjalistę.

Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektu.

Pakiet II

Dostawa licencji na urządzenia FortiWeb, FortiMail i FortiAnalyzer.

1) Odnowienie licencji na okres 3-4 lat (kryterium oceny oferty), upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów dla posiadanego przez zamawiającego rozwiązania FortiWeb-VM02, numer seryjny FVVM020000083423
   Powinny one obejmować:
   a) Kontrolę antywirusową, sygnatury ochrony dla aplikacji www oraz bazy reputacyjne adresów IP na okres 3-4 lat.
   b) Serwis producenta przez okres 3-4 lat upoważniający do aktualizacji oprogramowania oraz gwarancji w trybie 24x7
2) Odnowienie licencji na okres 3-4 lat (kryterium oceny oferty), upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów dla posiadanego przez zamawiającego rozwiązania FortiMail-VM02, numer seryjny FEVM020000130018
   Powinny one obejmować:
   a) Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake na okres 3-4 lat.
   b) Serwis gwarancyjny producenta przez okres 3-4 lat, upoważniający do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
3) Odnowienie licencji na okres 3-4 lat (kryterium oceny oferty), upoważniające do korzystania z serwisów dla posiadanego przez zamawiającego rozwiązania FortiAnalyzer-VM 25GB VM numer seryjny FAZ-VM0000078583
   Powinny one obejmować serwis gwarancyjnym producenta przez okres 3-4 lat, upoważniający do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020 oraz ze środków budżetu Województwa Kujawsko-Pomorskiego i Partnerów Projektu.