STAROSTWO POWIATOWE
W ŚRODZIE ŚLĄSKIEJ
ul. Wrocławska 2
55-300 ŚRODA ŚLĄSKA
tel. 71 317 56 46 (7); 71 396 89 00 (30)
fax 71 317 56 49
NIP 913-14-47-812; Reg. 931934762

Środa Śląska, dn.07.07.2021 r.

Nr postępowania: IZPO.3433.11.2021

ZAPROSZENIE DO SKŁADANIA OFERT
NA DOSTAWĘ I WDROŻENIE 2 URZĄDZEŃ KLASY NEXT GENERATION FIREWALL, PRACUJĄCYCH W TRYBIE KLASTRA NIEZWODNOŚCIOWEGO

I.NAZWA I ADRES ZAMAWIAJĄCEGO:

Powiat Średzki
ul. Wrocławska 2, 55-300 Środa Śląska
Regon 931934762, NIP 913-15-29-763

II. OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest:

1. Dostawa i wdrożenie 2 urządzeń klasy Next Generation Firewall, pracujących w trybie klastra niezwodnościowego Urządzenia o parametrach zgodnych z pkt. 3.

2. Świadczenie wsparcia technicznego dla oferowanego Systemu zabezpieczeń przez okres 12 miesięcy. Przez wsparcie techniczne rozumie się usługi pomocy technicznej świadczone przez autoryzowany ośrodek pomocy technicznej producenta oraz dostęp do nowych wersji oprogramowania dla wszystkich typów urządzeń i systemu zarządzania; aktualizację baz sygnatur aplikacyjnych, aktualizację baz sygnatur IPS, AV, AntySpyware oraz aktualizację baz kategorii URL, aktualizację baz DNS oraz ochronę i aktualizację sygnatur DLP.

3.Wymagana minimalna funkcjonalność i parametry zaoferowanych urządzeń (szczegółowy opis przedmiotu zamówienia):

Urządzenia klasy Next Generation Firewall - **klaster**

1) Urządzenia muszą realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.
2) Urządzenia muszą zapewniać obsługę dla IPv6.
3) Urządzenia muszą zapewnić możliwość statycznej i dynamicznej translacji adresów NAT między IPv4 i IPv6.
4) Urządzenia nie mogą posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
5) Reguły zabezpieczeń firewall zgodnie z ustaloną polityką opartą o profile oraz obiekty. Polityki muszą być definiowane pomiędzy określonymi strefami bezpieczeństwa. Konsola zarządzania posiada możliwości automatycznej weryfikacji spójności i niesprzeczności wprowadzonej polityki bezpieczeństwa.
6) Urządzenia muszą zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. Oferowany System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona

Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i anty-spyware), filtracja plików, danych i URL.

7) Urządzenia muszą zapewnić możliwość wykluczenia z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie co najmniej: kategoryzacji stron URL, dodania własnych wyjątków.
8) Urządzenia muszą zapewnić możliwość skanowania całości ruchu pod kontem zaistnienia podatności, a nie wyłącznie wybranych próbek ruchu.
9) Urządzenia muszą identyfikować co najmniej 2500 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS m.in.: Skype, Gadu-Gadu, Tor, BitTorrent.
10) Urządzenia muszą zapewnić możliwość definiowania własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta.
11) Urządzenia muszą zapewnić możliwość dodania własnej lub zmiany predefiniowanej kategoryzacji URL.
12) Zamawiający wymaga dostarczenia urządzenia z licencjami/subskrypcjami pozwalającymi na realizację funkcjonalności podmieniania adresów domen uznanych za złośliwe na zdefiniowany adres lokalny w odpowiedziach na zapytania DNS w celu wykrycia hostów z sieci wewnętrznej które próbują nawiązać komunikacje ze złośliwymi domenami. W przypadku, gdy funkcjonalność jest oferowana jako subskrypcja czasowa, Zamawiający wymaga dostarczenia subskrypcji na min. 12 miesięcy.
13) Urządzenia muszą umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN.
14) Zamawiający wymaga dostarczenia urządzeń z licencjami/subskrypcjami pozwalającymi na realizację funkcjonalności wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS). W przypadku gdy funkcjonalność jest oferowana jako subskrypcja czasowa, Zamawiający wymaga dostarczenia subskrypcji na min. 12 miesięcy.
15) Zamawiający wymaga dostarczenia urządzeń z licencjami/subskrypcjami pozwalającymi na realizację funkcjonalności inspekcji antywirusowej, kontrolującej przynajmniej protokoły: SMTP, HTTP i HTTPS oraz podstawowe rodzaje plików. Baza AV musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny. W przypadku gdy funkcjonalność jest oferowana jako subskrypcja czasowa, Zamawiający wymaga dostarczenia subskrypcji na min. 12 miesięcy.
16) Zamawiający wymaga dostarczenia urządzeń z licencjami/subskrypcjami pozwalającymi na realizację funkcjonalności filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza kategorii stron musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny. W przypadku gdy funkcjonalność jest oferowana jako subskrypcja czasowa, Zamawiający wymaga dostarczenia subskrypcji na min. 12 miesięcy.
17) Urządzenia muszą umożliwiać definiowanie i przydzielanie innych profili ochrony (AV, IPS, AS, URL) dla aplikacji pracujących na tym samym porcie UDP lub TCP.
18) Urządzenia muszą umożliwiać definiowanie i przydzielanie odmiennych profili kontrolujących transfer różnych rodzajów plików dla aplikacji pracujących na tym samym porcie UDP lub TCP.
19) Urządzenia muszą transparentnie ustalać tożsamość użytkowników sieci w oparciu o Active Directory. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
20) Urządzenia muszą wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
21) Urządzenia muszą działać w trybie routera (tzn. w warstwie 3 modelu OSI) oraz w trybie transparentnym (tzn. w warstwie 2 modelu OSI). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych.

22) W architekturze rozwiązania musi występować moduł zarządzania i moduł przetwarzania danych.
23) System musi składać się z dwóch fizycznych urządzeń, które muszą posiadać możliwość pracy w konfiguracji odpornej na awarie (HA) w trybie Active-Passive i Active-Active.
24) Urządzenia muszą umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenia muszą umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
25) Urządzenia muszą pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej.
26) Interfejs administracyjny urządzeń musi być w języku polskim lub angielskim.
27) Urządzenia muszą być dostarczone jako dedykowane urządzenia zabezpieczeń sieciowych (appliance).
28) Urządzenia nie mogą znajdować się na liście „end-of-sale" oraz „end-of-support" producenta.
29) Każde z urządzeń musi posiadać: wbudowane co najmniej 8 portów Ethernet 10M/100M/1G.
30) Każde z urządzeń musi posiadać: wbudowany co najmniej: 1 port 10M/100M/1G Ethernet out-of-band management, 1 port konsoli RJ45, 1 port USB
31) Urządzenia muszą zapewniać wydajność przynajmniej 1,5 Gbps dla ruchu IPSec VPN.
32) Urządzenia muszą posiadać przepustowość w ruchu nie mniej niż 2,2 Gbps dla kontroli firewall z włączoną funkcją kontroli aplikacji oraz akceptować nie mniej niż 38 000 połączeń na sekundę. Przepustowość dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (ochrona Intrusion Prevention, antywirus, filtracja aplikacji i kategoryzacja URL) nie może być mniejsza niż 0,9 Gbps.
33) Urządzenia muszą obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenia muszą obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP i OSPF.
34) System musi posiadać możliwość podłączenia urządzeń firewall w klastrze pod scentralizowany system zarządzania
35) Zarządzanie Systemu musi odbywać się z linii poleceń (CLI) oraz z graficznej konsoli GUI. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Dopuszcza się, aby polityki mogły być tworzone tylko z graficznej konsoli GUI.
36) Urządzenia muszą być wyposażone w dedykowany port zarządzania out-of-band.
37) Urządzenia muszą posiadać funkcjonalność pozwalającą administratorowi urządzenia na konfigurację rodzaju pliku (min. exe, dll), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box".
38) W przypadku gdy urządzenia pozwalają na jednoczesną pracę dwu lub więcej administratorów musi istnieć wbudowany w system mechanizm umożliwiający jednemu z administratorów uzyskanie wyłączności na wprowadzanie zmian. W tym czasie pozostali zalogowani użytkownicy nie mogą być w stanie dokonać żadnych zmian w konfiguracji.
39) Urządzenia muszą umożliwiać przesyłanie logów do kilku zdefiniowanych serwerów Syslog. Administrator urządzenia musi mieć możliwość zdefiniowania, dla każdej reguły bezpieczeństwa, innego serwera Syslog.
40) Urządzenia muszą mieć możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesje w przypadku, gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.
41) Urządzenia muszą być fabrycznie nowe, aktualnie obecne w linii produktowej producenta.
42) Pomoc techniczna dla systemu musi być dostępna w Polsce i świadczona w języku polskim.
43) Serwis dostępu do najnowszej wersji oprogramowania, serwis sprzętowy i ewentualne licencje/subskrypcje na aktualizację bazy aplikacji muszą być ważne przynajmniej przez 12 miesięcy.

4.Wymagania dodatkowe

Urządzenia klasy Next Generation Firewall – dla wszystkich firewalli

1. Urządzenie powinno posiadać koncept konfiguracji kandydackiej, którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu w tym:
   a. Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian, których są autorami.
   b. Możliwość blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
2. Urządzenie powinno posiadać kategoryzację stron URL w oparciu o więcej niż jedną kategorię przypisaną do jednej strony (np. rodzaj URL'a, poziom ryzyka).
3. Urządzenie powinno posiadać możliwość analizy polityk bezpieczeństwa w ramach ich optymalizacji pod kątem występujących aplikacji w ramach narzędzia wbudowanego w firmware firewalla.
4. Urządzenie powinno posiadać funkcjonalność identyfikowania złośliwych zapytań DNS i realizowania funkcji DNS Sinkholing dla co najmniej: domen DGA, tunelowania informacji w ruchu DNS, dynamicznie hostowanych domen, domen złośliwych (malware,phishing), niedawno rejestrowanych.

III.OCENA OFERT

1. Zamawiający dokona oceny ofert, na podstawie następujących kryteriów oceny ofert:

Lp.	Nazwa kryterium	Znaczenie kryterium (w %)
1.	Cena	60%
2.	Termin dostawy	40%

Ad.1) Cena ofertowa K(c)

a) przyjmuje się, że najwyższą ilość punktów tj.60 pkt otrzyma najniższą wśród cen zawartych w ofertach,
b) ceny pozostałych ofert punktowane będą w oparciu o n/w wzór:

$$K(c) = \frac{C\ min}{C\ (x)} \times 100 \times 60\%$$

gdzie:
K(c)- oznacza ilość punktów przyznanych ofercie badanej „x" za kryterium ceny za wykonanie zamówienia
C min – cena brutto najniższa wśród cena zawartych w badanych ofertach
C (x) – cena brutto zawarta w ofercie badanej „x"

Ad.2) Termin dostawy K(t)

Termin dostawy liczony będzie w dniach i nie może być dłuższy niż 30 dni.

a) przyjmuje się, że oferta z terminem dostawy wynoszącym:

- 14 dni -otrzyma maksymalną ilość 40 punktów
- 21 dni -otrzyma 20 punktów
- 30 dni -otrzyma 1 punkt

- **ŁĄCZNA OCENA OFERTY:**

Zamawiający uzna za najkorzystniejszą ofertę, która uzyskała najwyższą ilość punktów za sumę wszystkich kryteriów wg wzoru:

W(x) = K(c) + K(t)
gdzie:
W(x) - wskaźnik oceny oferty badanej „x"
K(c) - ilość punktów przyznana ofercie badanej „x" za cenę ofertową
K(t) - ilość punktów przyznana ofercie badanej „x" za termin dostawy

Ocena punktowa oferty będzie zaokrąglona do dwóch miejsc po przecinku liczbą.

2. Wybór najkorzystniejszej oferty w przypadku jednakowej punktacji , oferty dodatkowe-
1) jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny lub kosztu i innych kryteriów oceny ofert, Zamawiający wybiera spośród tych ofert ofertę, która otrzymała najwyższą ocenę w kryterium o najwyższej wadze,
2) jeżeli oferty otrzymały taką samą ocenę w kryterium o najwyższej wadze, Zamawiający wybiera ofertę z najniższą ceną lub najniższym kosztem,
3) jeżeli nie można dokonać wyboru oferty w sposób, o którym mowa w ust. 2, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych zawierających nową cenę lub koszt.

IV. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1.Wykonawca może złożyć tylko 1 ofertę. Treść oferty musi odpowiadać treści niniejszego zaproszenia do składania ofert.
2. Ofertę składa się w formie elektronicznej, w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym. Oferta powinna być podpisana przez osobę upoważnioną do reprezentowania Wykonawcy zgodnie z formą reprezentacji Wykonawcy określoną w rejestrze lub innym dokumencie właściwym dla danej formy organizacyjnej Wykonawcy albo przez upełnomocnionego przedstawiciela Wykonawcy.
3. **Oferta musi zawierać :**
1) **formularz oferty** (załącznik nr 1),
2) **opis oferowanego przedmiotu zamówienia (parametry zaoferowanych urządzeń)** – stosownie do opisu w pkt. II ust.3 i 4.
3)upoważnienie osób podpisujących ofertę (jeżeli upoważnienie takie nie wynika wprost z odpisu z właściwego rejestru Wykonawcy) - do oferty należy dołączyć dokument ustanawiający pełnomocnika.

V. MIEJSCE I TERMIN SKŁADANIA OFERT.

Ofetę z wymaganymi dokumentami należy złożyć pod adresem e-mail :
informatyk.gkk@powiat-sredzki.pl

- do dnia 14 lipca 2021 r.

STAROSTA
Krzysztof Szałankiewicz