Ogłoszenie nr 510167379-N-2020 z dnia 03-09-2020 r.

Miasto Rybnik: Zakup i dostawa Firewall Miejskiej Sieci Szerokopasmowej

OGŁOSZENIE O UDZIELENIU ZAMÓWIENIA - Dostawy

Zamieszczanie ogłoszenia:
obowiązkowe
Ogłoszenie dotyczy:
zamówienia publicznego
Zamówienie dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej
nie
Zamówienie było przedmiotem ogłoszenia w Biuletynie Zamówień Publicznych:
tak
Numer ogłoszenia: 560294-N-2020
Ogłoszenie o zmianie ogłoszenia zostało zamieszczone w Biuletynie Zamówień Publicznych:
nie

SEKCJA I: ZAMAWIAJĄCY

I. 1) NAZWA I ADRES:
Miasto Rybnik, Krajowy numer identyfikacyjny 27625543000000, ul. Bolesława Chrobrego 2, 44-200 Rybnik, woj. śląskie, państwo Polska, tel. +48324392302, e-mail zam_pub@um.rybnik.pl, faks +48324224124.
Adres strony internetowej (url): www.rybnik.eu
I.2) RODZAJ ZAMAWIAJĄCEGO:
Administracja samorządowa

SEKCJA II: PRZEDMIOT ZAMÓWIENIA

II.1) Nazwa nadana zamówieniu przez zamawiającego:
Zakup i dostawa Firewall Miejskiej Sieci Szerokopasmowej
Numer referencyjny*(jeżeli dotyczy):*
ZP.271.45.2020
II.2) Rodzaj zamówienia:
Dostawy
II.3) Krótki opis przedmiotu zamówienia *(wielkość, zakres, rodzaj i ilość dostaw, usług lub robót budowlanych lub określenie zapotrzebowania i wymagań)* **a w przypadku partnerstwa innowacyjnego - określenie zapotrzebowania na innowacyjny produkt, usługę lub roboty budowlane:**
Przedmiotem zamówienia jest dostawa wraz z uruchomieniem dwóch urządzeń typu firewall na potrzeby Miejskiej Sieci Szerokopasmowej (MSS) na warunkach wskazanych poniżej. Realizacja przedmiotu zamówienia obejmuje: 1) dostawę firewall nowej generacji z licencją IPS – 2 urządzenia, 2) montaż ww. urządzeń, 3) przeniesienie konfiguracji z obecnie działających firewalli CISCO ASA 5540, 4) szkolenie z obsługi dla administratorów MSS, 5) świadczenie usług gwarancyjnych w oparciu o serwis producenta na okres 36-mc, w tym aktualizacja oprogramowania systemowego dostarczonych urządzeń. Architektura urządzenia, obudowa, interfejsy 1) Urządzenie będące dedykowaną platformą sprzętową – Zamawiający nie dopuszcza rozwiązań „serwerowych/wirtualnych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia. 2) Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall). 3) Urządzenie wyposażone w min. 8 portów SFP RJ45 oraz min. 4 porty SFP. 4) Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 1 000 sieci VLAN. 5) Urządzenie wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band . 6) Urządzenie wyposażone w port USB 3.0. 7) Zasilacz umożliwiający zasilanie prądem przemiennym 230V. 8) Możliwość montażu w szafie rack 19" (dołączone niezbędne elementy montażowe). 9) Wysokość urządzenia 1U. Parametry wydajnościowe 1) Przepustowość urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji (AVC) na poziomie min. 2 Gbps dla pakietów wielkości 1024B. 2) Przepustowość urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji (AVC) wraz z uruchomionym silnikiem IPS (Intrusion Prevention System) na poziomie min. 2 Gbps dla pakietów wielkości 1024B. 3) Min. 350 000 maksymalnych jednoczesnych sesji (z kontrolą aplikacji) z możliwością zestawiania co najmniej 20 000 nowych połączeń na sekundę. 4) Możliwość połączenia VPN do 400 urządzeń z maksymalną sumaryczną przepustowością min 1 Gbps dla pakietów 1024B TCP. 5) Przepustowość dekrypcji ruchu szyfrowanego (50% ruchu TLS 1.2, AES256-SHA z RSA 2048B) wynosi min. 1 Gbps. 6) Maksymalna ilość „wirtualny/logiczno firewalla" – 5, przy dostawie urządzenia należy dostarczyć 2 dla każdego urządzenia. Funkcjonalność urządzenia 1) Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej. 2)

Możliwość uruchomienia urządzenia w trybie firewall'a L3, jak i w trybie transparentnym. 3) Urządzenie obsługuje routing statyczny i dynamiczny (RIP, OSPF, BGP) . 4) Urządzenie umożliwia separację ruchu w warstwie L3 w ramach jednej instancji firewalla poprzez tworzenie osobnych tablic routingu. 5) Urządzenie umożliwia utworzenia min. 2 tablic rutingu. 6) Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory. 7) Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT). 8) Urządzenie może pracować w układzie wysokiej dostępności (HA) active/standby. 9) Urządzanie zapewnia możliwość obsługi użytkowników zdalnych VPN (RA VPN). 10) Urządzenie zapewnia funkcjonalności: a) systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control), b) systemu IPS, c) systemu ochrony przed malware, d) systemu filtracji ruchu w oparciu o URL, 11) Wraz z urządzeniem należy dostarczyć licencję/subskrybcję systemu IPS na min. 3 lata. 12) System posiada możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System ma tworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów: a) wiedza o użytkownikach – uwierzytelnienie, b) wiedza o urządzeniach – pasywne skanowanie ruchu, c) wiedza o urządzeniach mobilnych, d) wiedza o aplikacjach wykorzystywanych po stronie klienta, e) wiedza o podatnościach, f) wiedza o bieżących zagrożeniach, g) baza danych URL. 13) System posiada otwarte API dla współpracy z systemami zewnętrznymi. 14) Rozwiązanie współpracuje z systemami SIEM (Security Information and Event Management). 15) System wykrywania aplikacji AVC zapewniający: a) możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji, b) możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług, c) wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji, d) współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach. 16) System IPS zapewniający: a) możliwość pracy w trybie in-line, b) możliwość pracy w trybie pasywnym (IDS), c) możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym: - złośliwe oprogramowanie, - skanowanie sieci, - ataki na usługę VoIP, - próby przepełnienia bufora, - ataki na aplikacje P2P, - zagrożenia dnia zerowego, d) możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna), e) wiele sposobów wykrywania zagrożeń w tym: - sygnatury ataków opartych na exploitach, - reguły oparte na zagrożeniach, - mechanizm wykrywania anomalii w protokołach, - mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego, f) możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu, g) mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives), h) możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń, i) wiele możliwości reakcji na zdarzenia w tym takie, jak: - tylko monitorowanie, - blokowanie ruchu zawierającego zagrożenia, - zastąpienie zawartości pakietów, - zapisywanie pakietów, j) możliwość detekcji ataków i zagrożeń opartych na protokole IPv6, k) możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o: - systemach operacyjnych, - serwisach, - otwartych portach, aplikacjach , - zagrożeniach, l) możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych, m) możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp., n) możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji, o) możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego, p) mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne, q) możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie, r) obsługę reguł system wykrywania włamań Snort, s) możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS, t) mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise), u) mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa. 17) System filtracji URL zapewniający: a) kategoryzację stron – w co najmniej 80 kategoriach, b) bazę URL o wielkości nie mniejszej niż 280 mln URL, c) bazę URL producenta rozwiązania. 18) Urządzenie zapewnia możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym: a) pliki systemowe, b) pliki graficzne, c) pliki PDF, d) pliki wykonywalne, e) pliki multimedialne, f) pliki pakietu Office, g) pliki skompresowane. 19) Urządzenie posiada możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download. 20) Wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez: a) sprawdzenie reputacji plików w systemie globalnym, b) sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze), c) statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu. 21) Urządzenie zapewnia możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach: a) pliki wolne od złośliwego kod, b) pliki zawierające złośliwy kod, c) pliki podejrzane, d) pliki o własnej, zdefiniowanej przez użytkownika kategorii. 22) Podsystem wykrywania oprogramowania złośliwego zawiera narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna). Zarządzanie

urządzeniem Wraz z urządzeniem Wykonawca zobowiązany jest dostarczyć dedykowaną platformę zarządzającą opartą na dedykowanym, uodpornionym (ang. hardened) systemie operacyjnym. Platforma zarządzająca może mieć formę maszyny wirtualnej pracującej pod kontrolę Kernel Based Virtual Machines (KVM) i spełnia następujące wymagania: 1) umożliwia agregację wszystkich zdarzeń IDS/IPS oraz centralne monitorowanie i analizę działającą w czasie rzeczywistym, 2) jest dostępna przez interfejs WEB, bez potrzeby instalacji dodatkowego oprogramowania klienckiego, 3) zapewnia interfejs, który może zostać dostosowany do wymagań użytkownika, w szczególności administrator posiada możliwość definiowania widoków (dashboard), które spełniają jego indywidualne kryteria, 4) ma możliwość konfigurowania limitu powtórzeń danego zdarzenia w określonym czasie zanim zostanie wygenerowany alarm, 5) ma możliwość automatycznej konfiguracji pobierania zestawów sygnatur na najnowsze zagrożenia i podatności. Ma możliwość informowania o zmianach w pakietach z nowymi sygnaturami/regułami, 6) zapewnia zarządzanie oparte o role, gdzie każdy z użytkowników systemu może mieć różne widoki interfejsu oraz różne możliwości konfiguracyjne w zależności od roli, do której został przypisany, 7) zapewnia funkcjonalność typu harmonogram zadań umożliwiającą automatyczne uruchamianie rutynowych czynności administracyjnych takich jak kopie zapasowe, uaktualnienia, tworzenie raportów, stosowanie polityk bezpieczeństwa oraz automatyczne dostrajanie polityki IPS, 8) zapewnia grupowanie urządzeń i polityk w celu ułatwienia zarządzania konfiguracją, 9) ma możliwość przechowywania atrybutów hostów definiowanych przez użytkownika takich jak jego krytyczność tak, aby ułatwić czynności monitorowania sieci, 10) daje możliwość znaczącej redukcji nakładów operacyjnych oraz przyśpieszenie reakcji na zagrożenia poprzez automatyczną priorytetyzację alarmów w oparciu o korelację zagrożeń ze skutecznością ataku na docelowego hosta, 11) ma możliwość dynamicznego dostrajania systemu IDS/IPS przy zachowaniu minimalnej interwencji administratora, 12) zapewnia możliwość automatycznego uaktualniania reguł publikowanych przez producenta, automatyczną dystrybucję i stosowanie reguł na urządzeniach IPS, 13) ma możliwość wykonywania i odtwarzania kopi zapasowych zarówno urządzeń bezpieczeństwa, jak i platformy zarządzającej, 14) zapewnia funkcjonalność pozwalającą na zarządzanie cyklem życia incydentu, od początkowego powiadomienia, poprzez odpowiedzi, aż do rozwiązania, 15) zapewnia możliwość wglądu w reguły, które wygenerowały dany incydent oraz powiązanego z nim pakietu, 16) zapewnia możliwość synchronizowania czasu pomiędzy wszystkimi komponentami przez protokół NTP, 17) zapewnia możliwość logowania wszystkich czynności wykonywanych przez administratora zarówno lokalnie jak i na zdalnym serwerze, 18) zapewnia szerokie możliwości generowania raportów włączając w to raporty predefiniowane oraz możliwość kompletnego dostosowania raportów do wymagań użytkownika, 19) zapewnia informowanie o zagrożeniach poprzez: a) wysłanie e-maila, b) wyslanie trap SNMP, c) przesłanie informacji do serwera Syslog, d) uruchomienie skryptu użytkownika, e) wysłanie informacji do jednego lub kilku rozwiązań typu SIEM poprzez zaszyfrowane łącze. 20) posiada zaawansowany system przeszukiwania logów pozwalający na przeprowadzanie analizy: a) aktualnego stanu danego urządzenia, b) podglądu historii dostępnych zasobów, c) możliwość eliminacji powtarzających się alarmów (tzw. Black Listing). 21) ma możliwość ustanawiania i wymuszania polityki zgodności jak i alarmowania w przypadku jej naruszeń w czasie rzeczywistym, 22) ma możliwość przypisywania następujących parametrów w polityce kontroli dostępu dla danych interfejsów, podsieci, vlanów i użytkowników: a) dozwolone porty i protokoły, b) dozwolone aplikacje według różnych kategorii, c) dozwolone kategorie stron internetowych (URL filtering), d) dedykowaną politykę wykrywania zagrożeń IPS dla każdej z reguł zapory ogniowej, e) sposób traktowania wyspecyfikowanego ruchu w danej regule: przepuszczanie bez analizy, analiza, blokowanie ciche, blokowanie z resetowaniem sesji, blokowanie interaktywne. 23) w ramach funkcji kategoryzacji zapytań HTTP (URL filtering) rozwiązanie ma możliwość interaktywnego blokowania z resetowaniem zapytań. W ramach tej funkcji jest zapewniona możliwość zdefiniowania własnej strony internetowej ostrzegającej o naruszeniu polityki kontroli dostępu i zrzuceniu zablokowanej próby połączenia. 24) posiada wbudowany edytor reguł IPS w formacie Snort oraz własnych detektorów aplikacji w języku LUA, 25) posiada wbudowane narzędzie do obsługi informacji o zagrożeniach z wielu źródeł poprzez STIX/TAXII, importu przez URL oraz uploadu z lokalnego komputera. Zgodnie z art. 30 ust 5 ustawy wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest zobowiązany wykazać, że oferowane przez niego dostawy, usługi lub roboty budowlane spełniają wymagania określone przez Zamawiającego.

II.4) Informacja o częściach zamówienia:

Zamówienie było podzielone na części:

nie

II.5) Główny Kod CPV: 32420000-3

Dodatkowe kody CPV: 32410000-0

SEKCJA III: PROCEDURA

III.1) TRYB UDZIELENIA ZAMÓWIENIA

Przetarg nieograniczony

III.2) Ogłoszenie dotyczy zakończenia dynamicznego systemu zakupów

nie

III.3) Informacje dodatkowe:

SEKCJA IV: UDZIELENIE ZAMÓWIENIA

IV.1) DATA UDZIELENIA ZAMÓWIENIA: 26/08/2020

IV.2) Całkowita wartość zamówienia

Wartość bez VAT 150000.00

Waluta PLN

IV.3) INFORMACJE O OFERTACH

Liczba otrzymanych ofert: 2

w tym:

liczba otrzymanych ofert od małych i średnich przedsiębiorstw: 1

liczba otrzymanych ofert od wykonawców z innych państw członkowskich Unii Europejskiej: 0

liczba otrzymanych ofert od wykonawców z państw niebędących członkami Unii Europejskiej: 0

liczba ofert otrzymanych drogą elektroniczną: 0

IV.4) LICZBA ODRZUCONYCH OFERT: 1

IV.5) NAZWA I ADRES WYKONAWCY, KTÓREMU UDZIELONO ZAMÓWIENIA

Zamówienie zostało udzielone wykonawcom wspólnie ubiegającym się o udzielenie:

tak

Nazwa wykonawcy: NTT Poland Sp. z o.o.

Email wykonawcy: kontakt.pl@global.ntt

Adres pocztowy: ul. Sienna 7

Kod pocztowy: 00-833

Miejscowość: Warszawa

Kraj/woj.: mazowieckie

Wykonawca jest małym/średnim przedsiębiorcą:

nie

Wykonawca pochodzi z innego państwa członkowskiego Unii Europejskiej:

nie

Wykonawca pochodzi z innego państwa nie będącego członkiem Unii Europejskiej:

nie

IV.6) INFORMACJA O CENIE WYBRANEJ OFERTY/ WARTOŚCI ZAWARTEJ UMOWY ORAZ O OFERTACH Z NAJNIŻSZĄ I NAJWYŻSZĄ CENĄ/KOSZTEM

Cena wybranej oferty/wartość umowy 99705.00

Oferta z najniższą ceną/kosztem 99705.00

Oferta z najwyższą ceną/kosztem 113000.00

Waluta: PLN

IV.7) Informacje na temat podwykonawstwa

Wykonawca przewiduje powierzenie wykonania części zamówienia podwykonawcy/podwykonawcom

nie

Wartość lub procentowa część zamówienia, jaka zostanie powierzona podwykonawcy lub podwykonawcom:

IV.8) Informacje dodatkowe:

IV.9) UZASADNIENIE UDZIELENIA ZAMÓWIENIA W TRYBIE NEGOCJACJI BEZ OGŁOSZENIA, ZAMÓWIENIA Z WOLNEJ RĘKI ALBO ZAPYTANIA O CENĘ

IV.9.1) Podstawa prawna

Postępowanie prowadzone jest w trybie na podstawie art. ustawy Pzp.

IV.9.2) Uzasadnienie wyboru trybu

Należy podać uzasadnienie faktyczne i prawne wyboru trybu oraz wyjaśnić, dlaczego udzielenie zamówienia jest zgodne z przepisami.