Gmina Nysa
Urząd Miejski w Nysie - ul. Kolejowa 15, 48-300 Nysa

BZP.271.**8**.2025 Nysa, dnia 12 marca 2025 r.

Strona internetowa prowadzonego postępowania

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez negocjacji pn.: **Wymiana systemu zapór sieciowych w Urzędzie Miejskim w Nysie,** *w ramach realizacji projektu Cyberbezpieczny Samorząd - Gmina Nysa (umowa o powierzenie grantu: FERC.02.02-CS.01-001/23/0675/ FERC.02.02-CS.01-001/23/2024 z 04.06.2024 r.)*

WYJAŚNIENIA TREŚCI SWZ

Zgodnie art. 284 ust. 2 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Pzp.), Zamawiający udziela wyjaśnień na zapytania dotyczące treści specyfikacji warunków zamówienia dla przedmiotowego postępowania.

Pytanie nr 1:
Czy Zamawiający dopuści rozwiązanie, które będzie posiadać wbudowane:
a) co najmniej 12 portów 1-Gigabit Ethernet RJ45,
b) co najmniej 4 porty 1 Gigabit Ethernet SFP oraz co najmniej 6 portów 10 Gigabit Ethernet SFP+ obsługujące moduły optyczne SR oraz LR, dla którym prędkość można obniżyć stosując moduły optyczne SFP
c) co najmniej 1 port 1-Gigabit Ethernet RJ45 wyłącznie do celów zarządzania,
d) co najmniej 1 port konsolowy,
e) co najmniej dwa porty 1-Gigabit Ethernet RJ45. Porty te muszą być traktowane jako dodatkowe względem wymaganych przez Zamawiającego. Nie dopuszcza się wykorzystania do celu klastrowania portów opisanych w podstawowych wymaganiach.
f) Wolny jednej moduł rozszerzeń o dodatkowe karty, gdzie zamawiający może zainstalować nawet porty 40GE QSFP+

Odpowiedź:
Zamawiający nie dopuszcza proponowanego rozwiązania.

Pytanie nr 2:
Czy Zamawiający wyrazi zgodę za dopuszczenie rozwiązania, które będzie spełniać co najmniej następujące parametry:
3.6 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: włączone wszystkie sygnatury IPS, antywirus, antyspyware, blokowanie typów plików, z włączonym logowaniem na dyski urządzenia - przy transakcjach 64KB
3.5 Gbps dla IPSec VPN

Odpowiedź:
Zamawiający nie dopuszcza proponowanego rozwiązania.

Pytanie nr 3:
Czy Zamawiający dopuści rozwiązanie, które będzie w ramach dostarczonej licencji posiadać co najmniej 10 wirtualnych instancji firewall (określanych jako kontekst/domena/system). Każda z instancji musi pozwalać na konfigurację niezależnych oraz odrębnych od innych instancji - tablicy routingu oraz *działać bez polityk bezpieczeństwa jak IPS, AV*

Odpowiedź:
Zamawiający wyraża zgodę na zaproponowane rozwiązanie, pod warunkiem spełnienia pozostałych wymaganych minimalnych parametrów technicznych określonych w Opisie przedmiotu zamówienia dla komponentu (element/cecha) - *„Wirtualizacja”.*

Pytanie nr 4:
Urządzenie musi wykrywać co najmniej 4000 predefiniowanych aplikacji wspieranych przez producenta (takich jak: DNS over HTTPS, Telegram, Skype, Tor, BitTorrent, MQTT, Modbus, DNP3, Siemens S7) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.
Pytanie: Czy Zamawiający dopuści rozwiązanie, które nie będzie wspierało DNS over HTTPS DNP3, Siemens S7?
Odpowiedź:
Zamawiający nie dopuszcza proponowanego rozwiązania.

Pytanie nr 5:
Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: .pif,
.scr, .cpl, .dll, .ocx, .exe, .class, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku
Pytanie: Czy Zamawiający dopuści rozwiązanie, które nie będzie wspierało szyfrowany MS Office, szyfrowanego RAR, szyfrowany ZIP ale będzie w stanie rozpakować i przeanalizować archiwum do 16 podpoziomów skompresowania?
Odpowiedź:
Zamawiający nie dopuszcza proponowanego rozwiązania.

Pytanie nr 6:
Urządzenie musi posiadać możliwość odnotowywania wykonywania operacji odszyfrowania ruchu w logach urządzenia w dedykowanej do tego celu sekcji. Logi muszą zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.
Pytanie: Czy Zamawiający dopuści rozwiązanie, które nie będzie wspierało mechanizmu automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu ale możliwość ręcznego dodawania wykluczania z szyfrowania problematycznych stron np. importując je z pliku csv?
Odpowiedź:
Zamawiający nie dopuszcza proponowanego rozwiązania.

Pytanie nr 7:
Urządzenie musi zapewniać inspekcję komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu blokowania tunelowania SSH.
Pytanie: Czy Zamawiający dopuści rozwiązanie, które nie będzie wspierało inspekcję komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu blokowania tunelowania SSH.
Odpowiedź:
Zamawiający nie dopuszcza proponowanego rozwiązania.

Pytanie nr 8:
Urządzenie musi posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół (co najmniej: http, http2, smtp, imap, pop3, ftp, smb). Baza sygnatur antywirusa musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż raz na 48 godzin i pochodzić od tego samego producenta co urządzenie.
Pytanie: Czy Zamawiający dopuści rozwiązanie, które będzie miało inspekcję antywirusowa w oparciu o AI, z ograniczeniem dla tradycyjnych silników AV. Dzięki takiemu silnikowi, rozwiązanie skuteczniej wykrywa wszystkie znane i nieznane zagrożenia
Odpowiedź:
Zamawiający wyraża zgodę na zaproponowane rozwiązanie, pod warunkiem spełnienia pozostałych wymaganych minimalnych parametrów technicznych określonych w Opisie przedmiotu zamówienia dla komponentu (element/cecha) - *„Funkcjonalności”.*

Pytanie nr 9:
Urządzenie musi posiadać funkcję antispyware. Baza sygnatur musi być przechowywana na dostarczonych urządzeniach, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co urządzenie.
Pytanie: Czy Zamawiający dopuści rozwiązanie, które będzie miało inspekcję antispyware oparciu o silnik AI, z ograniczeniem dla tradycyjnego silnik antispyware. Dzięki takiemu silnikowi, rozwiązanie skuteczniej wykrywa wszystkie znane i nieznane zagrożenia
Odpowiedź:
Zamawiający wyraża zgodę na zaproponowane rozwiązanie, pod warunkiem spełnienia pozostałych wymaganych minimalnych parametrów technicznych określonych w Opisie przedmiotu zamówienia dla komponentu (element/cecha) - *„Funkcjonalności".*

Pytanie nr 10:
Urządzenie musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sandbox" plików różnych typów (co najmniej: Windows Portable Executable (m.in. exe, dll), MacOS (MachO, DMG, PKG), Linux ELF, pdf, MS Office, JAR, APK, JS, VBS, PowerShell Script, BAT, HTA) w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować urządzenie sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze docelowym po ataku. Interwał aktualizacyjny to maksymalnie 2 godziny
Pytanie: Czy Zamawiający dopuści rozwiązanie, które będzie wspierało MacOS (MachO, DMG, PKG), Linux ELF zamiast tego mogło budować własne listy wspierany plików do analizy?
Odpowiedź:
Zamawiający nie dopuszcza proponowanego rozwiązania.

Pytanie nr 11:
Urządzenie musi posiadać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
a) LDAP,
b) Microsoft Active Directory,
c) Microsoft Exchange,
d) Syslog,
e) RADIUS,
f) TACACS+.
Pytanie: Czy Zamawiający dopuści rozwiązanie, które będzie wspierało Microsoft Exchange, Syslog, TACACS+, zamiast tego będzie wspierało POP3 i budowanie uwierzytelniania SSO za pomocą Proxy, Pop3, Web i tworzenie captive portalu dla użytkowników?
Odpowiedź:
Zamawiający nie dopuszcza proponowanego rozwiązania.

Pytanie nr 12:
Urządzenie musi pozwalać na zapisanie raportów i ich uruchamianie w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
Pytanie: Czy zamawiający dopuści rozwiązanie, które będzie wspierało wynik działania raportów dostępny w formatach co najmniej PDF z możliwością dostosowania wyglądu oraz modyfikacji pól raportu?
Odpowiedź:
Zamawiający wyraża zgodę na zaproponowane rozwiązanie, pod warunkiem spełnienia pozostałych wymaganych minimalnych parametrów technicznych określonych w Opisie przedmiotu zamówienia dla komponentu (element/cecha) - *„Zarządzanie".*

Pytanie nr 13:
Urządzenie musi posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP oraz etykietach (tagi) dla środowiska VMware ESX i VMware vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można następnie wykorzystywać w polityce bezpieczeństwa urządzeń.
Pytanie: Czy Zamawiający dopuści rozwiązanie, które nie be posiadać funkcji dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP oraz etykietach (tagi) dla środowiska VMware ESX i VMware vCenter?
Odpowiedź:
Zamawiający nie dopuszcza proponowanego rozwiązania.

Przedmiotowe wyjaśnienia treści SWZ, stanowią integralną jej część, są wiążące dla wszystkich Wykonawców i należy je uwzględnić przy sporządzaniu i składaniu ofert.

Z up. BURMISTRZA

Piotr Bobak
SEKRETARZ MIASTA