

ZAŁĄCZNIK nr 1 do Zapytania ofertowego 38/11/2025

Opis przedmiotu zamówienia (OPZ)**Router posiadający zdolność do bezpiecznej integracji systemów OT z Internetem – 1 szt.**

Przedmiotem zamówienia jest dostawa **Routera posiadającego zdolność do bezpiecznej integracji systemów OT z Internetem – zwanym dalej System NGFW**.

Zaoferowany przedmiot postępowania oraz wszystkie jego części składowe muszą być nowe.

Zamawiający posiada w zasobach firmowych router CISCO FirePower 1140 NGFW Appliance - stąd dostarczone rozwiązanie systemowe w ramach postępowania musi być kompatybilne z aktualnie posiadanym w celu zapewnienia ciągłości bezpieczeństwa sieciowego i kompatybilności urządzeniowej.

ROZWIĄZANIA RÓWNOWAŻNE

Zamawiający dopuszcza składanie ofert równoważnych, spełniających warunki dotyczące przedmiotu zamówienia zawarte w niniejszym zapytaniu.

W każdym przypadku użycia w OPZ norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, Wykonawca powinien przyjąć, że odniesieniu takiemu towarzyszą wyrazy „lub równoważne”. W przypadku użycia w OPZ odniesień do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych Zamawiający dopuszcza rozwiązania równoważne z opisywanym. Wykonawca analizując OPZ powinien założyć, że każdemu odniesieniu użytemu w dokumentacji projektowej towarzyszy wyraz „lub równoważne”. W przypadku, gdy w OPZ zostały użyte znaki towarowe, oznacza to, że są podane przykładowo i określają jedynie minimalne oczekiwane parametry jakościowe oraz wymagany standard. Wykonawca może zastosować materiały lub urządzenia równoważne, lecz o parametrach technicznych i jakościowych podobnych lub lepszych, których zastosowanie w żaden sposób nie wpłynie negatywnie na prawidłowe funkcjonowanie rozwiązań przyjętych w OPZ. Wykonawca, który zastosuje urządzenia lub materiały równoważne będzie obowiązany wykazać w trakcie realizacji zamówienia, że zastosowane przez niego urządzenia i materiały spełniają wymagania określone przez Zamawiającego.

W przypadku, gdy w opisie przedmiotu zamówienia podano nazwy materiałów, produktów lub urządzeń konkretnych producentów to należy traktować to jedynie jako określenie pożądanego standardu i jakości. W przypadku zaoferowania rozwiązania równoważnego, Oferent zobowiązany jest wykazać równoważność zastosowanych rozwiązań.

Oferent zobowiązany jest załączyć do oferty:

- Specyfikację techniczną urządzenia oraz opis funkcjonalny systemu potwierdzającą spełnienie wymagań technicznych i funkcjonalnych
- Proponowane warunki gwarancyjne oraz warunki udzielenia licencji
- w przypadku złożenia oferty równoważnej, opis dokumentujący spełniania warunków zawartych w Opisie przedmiotu zamówienia
- OPZ z podpisanym oświadczeniem wg wzoru

WARUNKI GWARANCJI – okres min. 36 miesięcy

Maksymalny czas reakcji serwisu: 24h /next business day - w okresie gwarancji na przedmiot zamówienia (liczony od momentu zgłoszenia usterki do określenia przez Wykonawcę przyczyny usterki oraz sposobu i terminu jej usunięcia).

System NGFW (Next Generation FireWall) - Router posiadający zdolność do bezpiecznej integracji systemów OT z Internetem, składa się z następujących elementów:

- **Urządzenie NGFW** dostarczone jako dedykowane urządzenie i wraz ze wszystkimi usługami, wymagane licencje z okresem ważności min.3 lata
- **Konsola zarządzająca** dostarczona w postaci maszyny wirtualnej (oprogramowanie typu Firepower Managment Center lub równoważne –Zamawiający posiada w zasobach firmowych router CISCO FirePower 1140 NGFW Appliance - stąd dostarczone rozwiązanie systemowe w ramach postępowania musi być

kompatybilne z aktualnie posiadanym w celu zapewnienia ciągłości bezpieczeństwa sieciowego i kompatybilności urządzeniowej.)

I. Wymagania techniczne urządzenia:

NGFW -Architektura urządzenia:

1. Urządzenie będące dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych” 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 dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band
4. Urządzenie jest zasilane prądem przemiennym 230V
5. Możliwość montażu w szafie rack 19” (dołączone niezbędne elementy montażowe)
6. Urządzenie wyposażone w minimum 8 wbudowanych portów GbE RJ45, minimum 4 porty Gigabit Ethernet SFP
7. Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 1000 sieci VLAN
8. Urządzenie wyposażone w port USB 3.0
9. Wysokość urządzenia 1RU
10. Przepustowość urządzenia dla uruchomionych modułów firewall’a oraz kontroli aplikacji na poziomie minimum 3 Gbps dla pakietów wielkości 1024B.
11. Urządzenie osiąga powyższe parametry wydajnościowe również wraz z uruchomionym silnikiem IPS.
12. Minimum 400 000 maksymalnych jednoczesnych sesji (z kontrolą aplikacji) z możliwością zestawiania co najmniej 22 000 nowych połączeń na sekundę
13. Możliwość połączeń VPN do 400 urządzeń z maksymalną sumaryczną przepustowością 1.4 Gbps dla pakietów 1024B TCP
14. Przepustowość dekrpcji ruchu szyfrowanego (50% ruchu TLS 1.2, AES256-SHA z RSA 2048B) wynosi przynajmniej 1,2 Gbps
15. Urządzenie pozwala na utworzenie minimum 10 osobnych tablic routingu dla odseparowania ruchu na poziomie warstwy L3 dla grup interfejsów.

II. Opis funkcjonalny urządzenia:

1. Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
2. Możliwość uruchomienia urządzenia w trybie firewall’a L2 oraz L3
3. Urządzenie obsługuje routing statyczny oraz dynamiczny: RIP, OSPF, OSPFv3, BGP
4. Możliwość monitorowania dostępności „next hop” w trasach statycznych i automatycznego wyłączania trasy, gdy jest niedostępny.
5. Urządzenie obsługuje ruch multicastowy oraz protokoły IGMP, PIM-SM oraz bidirectional PIM
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 jako serwer DHCP lub DHCP relay oraz zapewnia usługę DDNS
9. Urządzenie może pracować w układzie wysokiej dostępności (HA) active/standby
10. Urządzenie zapewnia możliwość obsługi użytkowników zdalnych VPN (RA VPN)
11. Dla RA VPN urządzenie zapewnia integrację z systemami Multi-Factor Authentication MFA
12. Urządzenie umożliwia konfigurację tuneli VPN typu Site-to-Site w następujących topologiach:
 - a. Punkt-punkt
 - b. Gwiazda
 - c. Pełna siatka
13. Urządzenie zapewnia możliwość ograniczenia pasma w konkretnym kierunku – upload i download dla stref, IP, użytkowników, aplikacji, adresów URL i geolokacji.
14. System posiada możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie.
15. System posiada otwarte API dla współpracy z systemami zewnętrznymi
16. Rozwiązanie współpracuje z systemami SIEM
17. System posiada wbudowany moduł identyfikacji i kontroli aplikacji sieciowych, który zapewnia:
 - a. możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji sieciowych

- b. możliwość tworzenia profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego oraz wykorzystywanych usług
 - c. współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania aplikacji przez system oraz w regułach reagowania na zagrożenia i raportach
 - d. wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji
18. Urządzenie może być zarządzane lokalnie lub przez scentralizowaną konsolę zarządzającą
19. 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:
 - i. złośliwe oprogramowanie
 - ii. skanowanie sieci
 - iii. ataki na usługę VoIP
 - iv. próby przepełnienia bufora
 - v. ataki na aplikacje P2P
 - vi. zagrożenia dnia zerowego, itp.
 - 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:
 - i. sygnatury ataków opartych na exploitach
 - ii. reguły oparte na zagrożeniach
 - iii. mechanizm wykrywania anomalii w protokołach
 - iv. 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:
 - i. tylko monitorowanie
 - ii. blokowanie ruchu zawierającego zagrożenia
 - iii. zastąpienie zawartości pakietów
 - iv. 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:
 - i. systemach operacyjnych
 - ii. serwisach
 - iii. otwartych portach, aplikacjach
 - iv. 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 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, na podstawie danych kontekstowych
20. 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
21. Urządzenie posiada możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download
22. System umożliwia zdefiniowanie osobnej polityki IPS dla ruchu klasyfikowanego na podstawie aplikacji i wymagającego wymiany kilku pakietów w celu poprawnego wykrycia aplikacji.
23. System pozwala na budowanie polityk w oparciu o nazwy DNS z możliwością przekierowania zapytań do tzw. „sinkhole”.
24. System pozwala na przypisanie innych polityk IPS do różnych reguł polityki dostępu
25. System zbiera dane kontekstowe, na podstawie których buduje profil każdego hosta. Profil taki zawiera informacje o systemie operacyjnym i jego wersji, aplikacjach i ich wersjach, protokołach.
26. Wyżej wymienione dane kontekstowe są mapowane do wbudowanej bazy podatności na zagrożenia. Mapowanie pozwala na trafne określenie wpływu zagrożenia na zaatakowany system (jeżeli jest podatność system jest skompromitowany, jeżeli nie było podatności to system nie został skompromitowany).
27. System pozwala na wstrzykiwanie tagów usług Azure i AWS, tagów z Vmware oraz atrybutów Office365 i użycie ich w polityce bezpieczeństwa. System automatycznie reaguje na zmianę tych tagów i atrybutów bez konieczności aktualizowania polityki.
28. 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
29. Urządzenie zapewnia możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach:
- a. pliki wolne od złośliwego kodu
 - b. pliki zawierające złośliwy kod
 - c. pliki podejrzane
 - d. pliki o własnej, zdefiniowanej przez użytkownika kategorii
30. Podsystem wykrywania oprogramowania złośliwego zawiera narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna)

III. Opis funkcjonalny Systemu zarządzania urządzeniem (oprogramowanie typu Firepower Management Center na min. 2 urządzenia) – Konsoli Zarządzającej:

1. Wraz z urządzeniem zostanie dostarczona dedykowana platforma (konsola) zarządzająca oparta na dedykowanym, uodpornionym (ang. hardened) systemie operacyjnym. Platforma zarządzająca może mieć formę maszyny wirtualnej i spełniać następujące wymagania:
 - a. umożliwia agregację wszystkich zdarzeń IDS/IPS oraz centralne monitorowanie i analizę działającą w czasie rzeczywistym
 - b. jest dostępna przez interfejs WEB, bez potrzeby instalacji dodatkowego oprogramowania klienckiego

- c. zapewnia interfejs, który może zostać dostosowany do wymagań użytkownika, w szczególności administrator posiada możliwość definiowania widoków (dashboard), które spełniają jego indywidualne kryteria
- d. ma możliwość konfigurowania limitu powtórzeń danego zdarzenia w określonym czasie zanim zostanie wygenerowany alarm
- e. ma możliwość automatycznej konfiguracji pobierania zestawów sygnatur na najnowsze zagrożenia i podatności. Ma możliwość informowania o zmianach w pakietach z nowymi sygnaturami/regułami
- f. zapewnia grupowanie urządzeń i polityk w celu ułatwienia zarządzania konfiguracją
- g. ma możliwość wykonywania i odtwarzania kopii zapasowych zarówno urządzeń bezpieczeństwa, jak i platformy zarządzającej
- h. zapewnia funkcjonalność pozwalającą na zarządzanie cyklem życia incydentu, od początkowego powiadomienia, poprzez odpowiedzi, aż do rozwiązania
- i. zapewnia możliwość wglądu w reguły, które wygenerowały dany incydent oraz powiązanego z nim pakietu
- j. zapewnia możliwość synchronizowania czasu pomiędzy wszystkimi komponentami przez protokół NTP
- k. zapewnia możliwość logowania wszystkich czynności wykonywanych przez administratora zarówno lokalnie jak i na zdalnym serwerze
- l. zapewnia szerokie możliwości generowania raportów włączając w to raporty predefiniowane oraz możliwość kompletnego dostosowania raportów do wymagań użytkownika
- m. zapewnia informowanie o zagrożeniach poprzez
 - i. wysłanie e-maila,
 - ii. wysłanie trap SNMP,
 - iii. przesłanie informacji do serwera Syslog,
 - iv. wysłanie informacji do jednego lub kilku rozwiązań typu SIEM poprzez zaszyfrowane połączenie
- n. posiada zaawansowany system przeszukiwania logów pozwalający na przeprowadzanie analizy
 - i. aktualnego stanu danego urządzenia,
 - ii. podglądu historii dostępnych zasobów,
 - iii. możliwość eliminacji powtarzających się alarmów (tzw. Black Listing)
- o. ma możliwość przypisywania następujących parametrów w polityce kontroli dostępu dla danych interfejsów, podsieci, vlanów i użytkowników:
 - i. dozwolone porty i protokoły
 - ii. dozwolone aplikacje według różnych kategorii
 - iii. dedykowaną politykę wykrywania zagrożeń IPS dla każdej z reguł zapory ogniowej
 - iv. sposób traktowania wyspecyfikowanego ruchu w danej regule: przepuszczanie bez analizy, analiza, blokowanie ciche, blokowanie z resetowaniem sesji, blokowanie interaktywne
- p. pozwala na wysłanie na sensor tylko wybranych elementów modyfikowanej konfiguracji

OŚWIADCZENIE OFERENTA

Oferent deklaruje realizację zamówienia zgodnie z zapisami niniejszej specyfikacji przedmiotu zamówienia. ☐ TAK ☐ NIE

Oferuję dostawę routera marki, rok produkcji

.....2025 r.
 (data i czytelny podpis osoby upoważnionej do reprezentowania Oferenta)