

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Dostawa 3 sztuk urządzeń systemu IDS/IPS dla środowiska OT (urządzenia klasy UTM/NGFW do segmentacji i ochrony sieci przemysłowej), wraz z licencjami, gwarancją i wsparciem technicznym

Część nr 4 zamówienia – Zadanie nr 2 obszaru technicznego OT wniosku o dofinansowanie

1. Przedmiot zamówienia

1. Przedmiotem zamówienia jest dostawa 3 (trzech) sztuk fabrycznie nowych, nieużywanych i nieregenerowanych urządzeń realizujących funkcję systemu IDS/IPS dla środowiska OT – urządzeń klasy UTM/NGFW przeznaczonych do segmentacji i ochrony sieci przemysłowej (OT) Zamawiającego, w tym systemów SCADA i sterowników PLC wykorzystywanych przy zbiorowym zaopatrzeniu w wodę, wraz z kompletem licencji aktywujących wszystkie funkcje bezpieczeństwa opisane w niniejszym dokumencie, na okres minimum do 31.12.2026 r. lub na licencji wieczystej.
2. Urządzenia będą pracować na styku sieci IT/OT oraz pomiędzy segmentami sieci OT, dlatego kluczowym wymaganiem jest głęboka analiza protokołów przemysłowych przez moduł IPS oraz możliwość pracy w trybie transparentnym (bridge) bez przerywania komunikacji przemysłowej.
3. Wszystkie dostarczone urządzenia muszą być identyczne (ten sam producent i model), pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej oraz być objęte gwarancją producenta realizowaną na terenie Polski. W ramach dostawy Wykonawca przeprowadzi montaż oraz konfigurację wstępną urządzeń w zakresie uzgodnionym z Zamawiającym, zgodnie z zakresem usług przewidzianym dla danej części zamówienia.
4. Każde urządzenie musi spełniać łącznie wszystkie wymagania minimalne określone w pkt 3. Parametry wskazane w niniejszym OPZ stanowią wymagania minimalne – Zamawiający dopuszcza zaoferowanie urządzeń o parametrach lepszych (równoważność funkcjonalna).

2. Wymagania techniczne minimalne

OBSŁUGA SIECI

Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (FIREWALL)

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.

5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
6. Urządzenie ma umożliwiać filtrowanie również na poziomie warstwy 2 modelu OSI, tj. na podstawie adresów MAC.
7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS.
7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
9. Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

KSZTAŁTOWANIE PASMA (TRAFFIC SHAPING)

1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.

3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

1. Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również, żeby analiza sandboxingu była przeprowadzana przez firmy trzecie. W odniesieniu do urządzeń pracujących w segmentach sieci OT pozbawionych dostępu do Internetu dopuszcza się realizację ochrony antywirusowej wyłącznie lokalnie (bez analizy sandbox), przy zachowaniu pełnej funkcjonalności sandboxingu dla urządzeń posiadających dostęp do Internetu.
2. Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania).
3. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.
4. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.

WIRTUALNE SIECI PRYWATNE (VPN)

1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
2. Urządzenie ma wspierać co najmniej sieci VPN typu IPSec VPN.
3. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
4. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
5. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
6. Rozwiązanie ma umożliwiać wykorzystanie algorytmów post-quantowej kryptografii w szyfrowaniu IPSec w standardzie ML-KEM.

UWIERZYTELNIANIE

1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
 - a) lokalną bazę użytkowników (wewnętrzny LDAP),
 - b) zewnętrzną bazę użytkowników (zewnętrzny LDAP),
 - c) usługę katalogową Microsoft Active Directory.
2. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
3. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
4. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
5. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
6. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli IPSec, jak również logowania do webowego interfejsu administracyjnego i SSH.

ROUTING (TRASOWANIE)

1. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).

ADMINISTRACJA URZĄDZENIEM

1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem interfejsu graficznego.
2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez zaszyfrowany protokół HTTPS.
3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
6. Urządzenie ma umożliwiać zarządzanie z poziomu konsoli (SSH).
7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
14. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
15. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
16. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
 - a) manualnego eksportu do pliku w dowolnym momencie czasu,
 - b) automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu.
17. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.

18. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
19. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS oraz skanera antywirusowego.
4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
8. Urządzenie ma umożliwiać monitorowanie swojego stanu z wykorzystaniem protokołu SNMP w wersji 2 i 3.
9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

1. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
2. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
3. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
4. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
5. Urządzenie ma umożliwiać stworzenie różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny.
6. Urządzenie ma posiadać usługę DNS Proxy.
7. Urządzenie ma posiadać wsparcie dla Spanning Tree Protocol (RSTP/MSTP).
8. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
9. Urządzenie musi mieć możliwość wykorzystania REST API.
10. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

PARAMETRY SPRZĘTOWE

1. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD lub wyposażone w dysk twardy do zbierania logów.
2. Liczba portów Ethernet 2,5 Gbps – min. 8, konfigurowalne niezależnie.

3. Przepustowość Firewall (1518 bajtów UDP) – minimum 10 Gbps.
4. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 6 Gbps.
5. Przepustowość typu Threat Prevention – minimum 740 Mbps.
6. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 3 Gbps.
7. Obsługa interfejsów 802.1Q (VLAN) – minimum 350.
8. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 39 000 nowych sesji/sekundę.
9. Urządzenie ma być dostarczone wraz z dodatkowym zewnętrznym zasilaczem (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
10. Urządzenie musi być wyposażone w moduł TPM.

GWARANCJA I SERWIS

1. Urządzenie ma być objęte gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.