GK.272.3.50.2025.MP

Załącznik nr 1
do zapytania ofertowego

Router – 1 szt.

Komponent	Opis minimalnych parametrów
Konstrukcja	System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania. Rozwiązanie powinno być wyposażone w moduł kryptograficzny zgodny ze standardem FIPS 140-2. Urządzenie w obudowie typu desktop z możliwością montażu w szafie rack 19" (uchwyty montażowe w komplecie).
Tryby pracy	Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca)
Ilość chronionych hostów	System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej.
Przechowywanie danych logów	Rozwiązanie musi być wyposażone w co najmniej jeden dysk SSD służący m.in. do przechowywania logów i raportów bezpośrednio na urządzeniu.
Zasilanie	Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy (drugi zasilacz jako wyposażenie opcjonalne).
Pamięć RAM	Minimum 8GB
Pamięc wewnętrzna	Zainstalowany nośnik eMMC minimum 16GB
Liczba fizycznych interfejsów 2.5GE	Minimum 4
Wydajność Firewall nie mniej niż (Gbps)	9.9
Wydajność Firewall IMIX nie mniej niż (Gbps)	6.5
Wydajność IPS nie mniej niż (Gbps)	6
Interfejs	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym.
Certyfikat SSL interfejsu	Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA).
Uwierzytelnianie	Rozwiązanie powinno oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN.
Diagnostyka	Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter. Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.
Zarządzanie	Rozwiązanie powinno oferować wiersz poleceń dostępny z poziomu graficznego interfejsu administratora, portu konsolowego oraz za

	pośrednictwem protokołu SSH z uwierzytelnianiem przy użyciu kluczy RSA, DSA lub ECDSA o długości min. 2048 bitów.
Aktualizacja oprogramowania	Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). Informacja o dostępności nowej wersji powinna pojawiać się w Web GUI. Producent powinien oferować mechanizm automatycznego łatania wykrytych w oprogramowaniu systemowym podatności przez tzw. hotfixies, przy czym administrator powinien móc funkcjonalność tą wyłączyć.
Zarządzanie licencjami	Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu licencyjnego a synchronizacja subskrypcji powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami.
Zarządzanie interfejsami	Rozwiązanie powinno zapewniać możliwość zmiany nazw interfejsów sieciowych.
Czas trwania subskrypcji na jaki uruchamiane są poniższe funkcjonalności	36 miesięcy
Ochrona IPS	Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur. Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS. Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS.
Ochrona ATP (Advanced Threat Protection)	System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet.
Zabezpieczenie sieci Web	Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP.
Silniki antywirusowe	Rozwiązanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania. Dodatkowo rozwiązanie powinno umożliwiać uruchomienie silnika antywirusowego firmy trzeciej. System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek.
Inspekcja ruchu SSL/TLS	Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów. Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do

	TLS 1.2. Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP. Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443). Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web. Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen.
Filtr WEB	Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron Web oraz umożliwiać dodawanie własnych kategorii stron. Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól. System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowania treści komunikatu w tym dodania logo organizacji.
Lista aplikacji	Rozwiązanie powinno oferować bazę danych opisująca co najmniej 3000 aplikacji. Rozwiązanie powinno umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp.
Ochrona email	Rozwiązanie musi zapewnić ochronę poczty email w tym skanowanie protokołów SMTP, POP3, IMAP. Blokowanie spamu i malware. Wsparcie dla DKIM, SPF, spam greylisting. Wykrywanie linków phishingowych. Dostęp dla indywidualnych użytkowników do blokowania lub dopuszczania nadawców poprzez konfigurację list. Obsługa kwarantanny wraz z możliwością przeglądania elementów w kwarantannie przez użytkowników
Inne zagrożenia	Sprzęt powinien zapewnić rozwiązanie klasy Sandbox do ochrony przed zagrożeniami typu Zero-Day. Rozwiązanie będzie ofertować statyczną i dynamiczną analizę kody przesyłanego w ramach ruchu web czy email. Rozwiązanie umożliwi dodatkową inspekcję i detonację plików wykonywalnych (.exe, .com, .dll) oraz dokumentów (.doc, .docx, .docm, .rtf), plików PDF a także archiwów.

GK.272.3.50.2025.MP

Załącznik nr 1
do zapytania ofertowego

W ramach zakupu ww. sprzętu Zamawiający zamawia usługę wdrożenia, która ma obejmować kompleksowe przygotowanie, konfigurację i uruchomienie urządzenia w środowisku klienta, z uwzględnieniem:

1) Instalacji fizycznej urządzenia w lokalizacji klienta,
2) Konfiguracji podstawowej sieci (interfejsy WAN/LAN, routing, NAT),
3) Konfiguracja VLAN
4) Integracji z dynamicznym adresem IP (np. poprzez DDNS),
5) Wdrożenia polityk bezpieczeństwa zgodnych z wymaganiami klienta,
6) Aktywacji i konfiguracji licencji,
7) Konfiguracji VPN (dla zdalnego dostępu lub połączeń site-to-site),
8) Wdrożenia ochrony poczty e-mail (filtr antyspamowy, skanowanie załączników, ochrona przed phishingiem),
9) Testów poprawności działania i wydajności urządzenia,
10) Przeszkolenia administratora IT klienta z zakresu obsługi urządzenia i panelu sterowania.
11) Szacowany czas wdrożenia: 1–2 dni robocze (w zależności od złożoności środowiska i dostępności infrastruktury klienta).
12) Całość wdrożenia musi odbyć się na miejscu w siedzibie Zamawiającego w ustalonych i zaakceptowanych przez Zamawiającego ramach czasowych

Efekty wdrożenia

1) Urządzenie UTM w pełni zintegrowane z siecią klienta,
2) Aktywna ochrona sieci i poczty e-mail zgodna z najlepszymi praktykami bezpieczeństwa,
3) Gotowość do dalszego zarządzania i rozbudowy UTM
4) Dokumentacja wdrożeniowa (schemat konfiguracji, dane dostępowe, polityki bezpieczeństwa).

Signature Not Verified

Dokument podpisany przez Maria Pałucka
Data: 2025.08.29 12:57:29 CEST