

## Opis Przedmiotu zamówienia

<b>Przedłużenie subskrypcji dla Fortigate 200E lub równoważne, spełniające co najmniej poniższe wymagania (2 lata)</b>	2	04.02.2025 - 03.02.2027
<ul style="list-style-type: none"> <li>• Licencja Fortigate 200E Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web &amp; Video Filtering, Antispam Service, and FortiCare Premium) na 2 lata</li> </ul> <p><b>lub równoważne, spełniające co najmniej poniższe wymagania:</b></p> <ul style="list-style-type: none"> <li>• UTM musi zapewniać wszystkie wymagane funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład UTM były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</li> <li>• W ramach dostarczonego systemu UTM musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: routingu, firewall-a, IPSec VPN, antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu.</li> <li>• System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: <ul style="list-style-type: none"> <li>○ routera z funkcją NAT,</li> <li>○ transparentnym,</li> <li>○ monitorowania na porcie SPAN.</li> </ul> </li> <li>• UTM musi wspierać IPv4 oraz IPv6 w zakresie: <ul style="list-style-type: none"> <li>○ firewall,</li> <li>○ ochrony w warstwie aplikacji,</li> <li>○ protokołów routingu dynamicznego.</li> </ul> </li> <li>• W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.</li> <li>• W ramach postępowania system musi zostać dostarczony w postaci redundantnej.</li> <li>• Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</li> <li>• Monitoring stanu realizowanych połączeń VPN.</li> <li>• System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.</li> <li>• System realizujący funkcję Firewall musi dysponować minimum: <ul style="list-style-type: none"> <li>○ 18 portami Gigabit Ethernet RJ-45.</li> <li>○ 4 gniazdami SFP 1 Gbps.</li> </ul> </li> <li>• System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</li> <li>• W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.</li> <li>• W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 135.000 nowych połączeń na sekundę.</li> <li>• Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 512B.</li> <li>• Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.5 Gbps.</li> <li>• Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA1: nie mniej niż 9 Gbps.</li> </ul>		

- Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 6 Gbps.
- Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps.
- Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem AES256-SHA1) dla ruchu http – minimum 1 Gbps.
- W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
  - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
  - Kontrola Aplikacji.
  - Poufność transmisji danych - połączenia szyfrowane IPsec VPN oraz SSL VPN.
  - Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
  - Ochrona przed atakami - Intrusion Prevention System.
  - Kontrola stron WWW.
  - Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
  - Zarządzanie pasmem (QoS, Traffic shaping).
  - Analiza ruchu szyfrowanego protokołem SSL oraz SSH.
  - Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
- Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
- Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
- System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
  - Translację jeden do jeden oraz jeden do wielu.
  - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
- W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
- System musi umożliwiać konfigurację połączeń typu IPsec VPN. W zakresie tej funkcji musi zapewniać:
  - Wsparcie dla IKE v1 oraz v2.
  - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM)
  - Obsługa protokołu Diffiego-Hellman grup 19 i 20
  - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
  - Tworzenie połączeń typu Site-to-site oraz Client-to-Site.
  - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
  - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
  - Obsługa mechanizmów: IPsec NAT Traversal, DPD, XAuth
  - Mechanizm „Split tunneling” dla połączeń Client-to-Site
- System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
  - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
  - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
- Dla modułów: IPsec VPN oraz SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. Klient VPN musi umożliwiać weryfikację stanu bezpieczeństwa stacji zdalnej.
- Rozwiązanie powinno zapewniać funkcjonalność VTEP (VXLAN Tunnel End Point)
- W zakresie routingu rozwiązanie powinno zapewniać obsługę:
  - Routingu statycznego
  - Policy Based Routingu

- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
- System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
- System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
- Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
- System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
- Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
- System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
- Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
- Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
- Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
- System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
- Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
- Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
- Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
- Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
- Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
- Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
- W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware, phishing, spam, Dynamic DNS, proxy avoidance.
- Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
- Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
- System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
- Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
- System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
  - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
  - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
  - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
- Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
- Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

- Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
- Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
- Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
- System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
- System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
- System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
- System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
- W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
- Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
- Musi istnieć możliwość logowania do serwera SYSLOG.
- Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
  - ICSA lub EAL4 dla funkcji Firewall
  - ICSA lub NSS Labs dla funkcji IPS
  - ICSA dla funkcji IPSec VPN
  - ICSA dla funkcji SSL VPN
- W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:
  - Kontrola aplikacji, IPS, antywirus, antyspam, Web Filtering na okres 12 miesięcy