Załącznik Nr 4

OPIS PRZEDMIOTU ZAMÓWIENIA – „Dostawa urządzenia typu UTM"

Towar musi być zgodny, równoważny lub o wyższych parametrach technicznych z wymaganiami określonymi poniżej:

Towar typu: urządzenie typu UTM – 1 sztuka spełniający niżej wymienione wymogi:				
lp.	**-1-**		**-2-**	**-3-**
1.	**Opis obligatoryjnych (minimalnych) parametrów technicznych dotyczących urządzenia UTM**			
	Wymagania obligatoryjne	System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN		
		W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.		
		System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.		
		Monitoring stanu realizowanych połączeń VPN.		
		W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 50 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.		
		System musi być wyposażony w zasilanie AC.		
		W zakresie Firewall'a obsługa nie mniej niż 1400 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.		

		Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.		
		Przepustowość Firewall z włączoną funkcją kontroli aplikacji: nie mniej niż 1.7 Gbps.		
		Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.		
		Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 1.4 Gbps.		
		Wydajność skanowania z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.		
		Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 650 Mbps.		

		W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. 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. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.	
		W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.	
		Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.	

		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 oraz SSL VPN.		
		IPSec VPN - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.		
		IPSec VPN - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.		
		IPSec VPN - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.		
		IPSec VPN - Mechanizm „Split tunneling" dla połączeń Client-to-Site.		
		SSL VPN - Praca w trybie Portal oraz w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.		
		Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.		
		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 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.		

		Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.		
		System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.		
		System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.		
		Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.		
		System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.		
		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.		
		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.		
		Funkcja Kontroli Aplikacji - aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.		
		Funkcja Kontroli Aplikacji - baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.		

		Funkcja Kontroli Aplikacji - administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.		
		Moduł kontroli WWW musi korzystać z bazy zawierającej adresy URL pogrupowane w kategorie tematyczne.		
		Moduł kontroli WWW - w ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, Dynamic DNS, proxy.		
		Moduł kontroli WWW - administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.		
		W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.		
		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) 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.		
		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.		
		Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.		
		W ramach logowania system pełniący funkcję Firewall 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.		
		W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania przez okres minimum 12 miesięcy z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować : Kontrolę Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analizę typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.		

	Wymagania obligatoryjne	Wykonawca ma obowiązek zainstalować urządzenie w szafie 19” Zamawiającego oraz dokonać jego konfiguracji wedle wymogów Zamawiającego. Czynności te będą wykonywane w porozumieniu z Zamawiającym oraz pod nadzorem Zamawiającego. W szczególności należy wykonać: • Aktualizację oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. • Aktywację (jeśli wymagana) urządzenia na stronie internetowej producenta. • Aktywację (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email etc) • Zamawiający wymaga migracji istniejących polityk z dotychczas wykorzystywanego urządzeń oraz ich modyfikacja po uzgodnieniu z Zamawiającym. • Konfigurację routingów statycznych na firewallu, • Konfigurację polityki bezpieczeństwa (reguły dostępu dla ruchu z Internetu, do Internetu oraz między pozostałymi strefami) zgodnie z wytycznymi ze strony Zamawiającego, • Konfigurację filtracji stron WWW na podstawie kategorii oraz treści, • Integrację UTMa z systemem autoryzacji Microsoft Active Directory tak aby możliwa była identyfikacja użytkowników, • Konfigurację dostępu zdalnego SSL VPN (VPN Client, portal WebVPN) • Konfigurację SSL Decryption łącznie z instruktażem jak zainstalować certyfikaty na stacjach klienckich.		
		Wykonawca dostarczy wszystkie niezbędne osprzęty, licencje wymagane do uruchomienia urządzeń zgodnie z wymaganiami zawartymi w Umowie oraz w Załączniku nr 1 do Umowy w tym kable połączeniowe i zasilające.		
		Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.		

		Wykonawca w ramach zamówienia przeprowadzi szkolenie w języku polskim w formie warsztatów, dla co najmniej 1 osoby (pracownik Zamawiającego) w wymiarze minimum 7 godzin, obejmujące co najmniej zakres konfiguracji urządzeń oraz rozwiązywania problemów (debugging i troubleshooting). Szkolenie ma odbyć się w Urzędzie Miejskim w Krynicy-Zdroju w dniach roboczych (poniedziałek-piątek).		
		Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.		
2.	**Opis opcjonalnych (dodatkowych) parametrów technicznych dotyczących serwerów**		**Parametry oferowanego systemu ****	**Liczba punktów za spełnienie wymagania**
		System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.	TAK / NIE	2
		Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system	TAK / NIE	1
		Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.	TAK / NIE	1
		Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure • Google Cloud Platform (GCP). • OpenStack. • VMware NSX.	TAK / NIE	1

		IPSec VPN - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.	TAK / NIE	1
		Funkcje SD-WAN - System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.	TAK / NIE	2
		System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.	TAK / NIE	1
		Moduł kontroli WWW - funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.	TAK / NIE	1
		Moduł kontroli WWW - administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.	TAK / NIE	1
		Elementy systemu bezpieczeństwa muszą realizować logowanie 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.	TAK / NIE	1