Załącznik nr 1C do siwz

Część 3 – ROUTER Z FUNKCJAMI ZABEZPIECZAJACYMI

Opis przedmiotu zamówienia

Równoważność

1. W punktach, gdzie przedmiot zamówienia opisany jest poprzez wskazanie znaków towarowych, patentów lub pochodzenia źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi, jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania innych wykonawców, Zamawiający dopuszcza zastosowanie rozwiązań równoważnych w stosunku do opisanych w SIWZ, pod warunkiem, że będą one spełniały minimalne parametry funkcjonalne i techniczne opisane w SIWZ i w żadnym punkcie nie obniżą parametrów przedmiotu zamówienia określonych w SIWZ.
2. W sytuacji, gdy Wykonawca zaproponuje urządzenia lub funkcjonalności równoważne, zobowiązany jest wykonać na własny koszt i załączyć do oferty zestawienie wszystkich zaproponowanych urządzeń i funkcjonalności i wykazać ich równoważność w stosunku do urządzeń i funkcjonalności opisanych w SIWZ, ze wskazaniem nazwy, strony i pozycji w dokumentacji, których dotyczy.
3. Wszystkie zaproponowane przez Wykonawcę równoważne urządzenia lub funkcjonalności muszą:
   a. posiadać parametry techniczne i funkcjonalne nie gorsze od określonych w opisie przedmiotu zamówienia,
   b. posiadać stosowne dopuszczenia i atesty.
4. Opis zaproponowanych rozwiązań równoważnych musi być dołączony do oferty i musi być na tyle szczegółowy, aby Zamawiający przy ocenie oferty mógł ocenić spełnienie wymagań dotyczących ich parametrów technicznych oraz rozstrzygnąć, czy zaproponowane rozwiązania są równoważne. Na Wykonawcy spoczywa obowiązek wykazania, że zaoferowane przez niego urządzenia lub funkcjonalności są równoważne w stosunku do opisanych przez Zamawiającego.

Wymagania ogólne

1. Urządzenie musi być fabrycznie nowe, nieregenerowane oraz pochodzić z oficjalnego kanału sprzedaży producenta na teren Polski (wymagane oświadczenie producenta, że oferowany do przetargu sprzęt spełnia ten wymóg, dostarczane na wezwanie Zamawiającego).
2. Urządzenie powinno mieć zainstalowane najnowsze oprogramowanie rekomendowane przez producenta.
3. Gwarancja min 5 lat.

Zamówienie obejmuje sprzęt komputerowy o następujących parametrach (lub równoważny):

Lp.	Nazwa, rodzaj	Parametry techniczne	Liczba sztuk
	Router z funkcjami zabezpieczającymi	• System musi być dostarczony w postaci kompletnego rozwiązania oraz posiadać możliwość pracy w trybie active-active lub active-passive w przypadku tworzenia klastra urządzeń. • Urządzenie musi być wyposażone we wszystkie licencje/subskrybcje umożliwiające uruchomienie funkcjonalności wyszczególnionych w poniższym opisie. Wszystkie komponenty muszą pochodzić od jednego producenta. • Urządzenie musi umożliwiać zdefiniowanie co najmniej 3 stref bezpieczeństwa • Urządzenie musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF i BGP • Urządzenie musi obsługiwać policy-based routing • Urządzenie musi obsługiwać adresację statyczną i dynamiczną (DHCP i PPPoE) na interfejsie zewnętrznym • Urządzenie musi obsługiwać adresację DHPCv6 na interfejsie zewnętrznym • Urządzenie musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP), jako bridge (transpartent mode) lub z tym samym adresem IP na wszystkich portach. • Urządzenie musi mieć możliwość obsługi wielu łączy	**1**

		zewnętrznych z opcją balansowania ruchu. • Urządzenie musi mieć możliwość obsługi łącza zapasowego typu LTE • Urządzenie musi obsługiwać Dynamic DNS (DDNS) • Urządzenie musi obsługiwać translację adresów: statyczną, dynamiczną i 1-to-1 • Urządzenie musi obsługiwać translację portów: PAT • Urządzenie musi obsługiwać IPSec NAT traversal • Urządzenie musi obsługiwać mechanizm policy-based NAT • Urządzenie musi obsługiwać VLAN (IEEE 802.1Q) • Urządzenie musi zapewniać ochronę przed atakami stosującymi techniki inwazyjne, np. fragmentacja pakietów • Urządzenie musi obsługiwać pracę jako serwer DHCP (IPv4 i IPv6) dla wszystkich interfejsów sieciowych segmentu LAN. • Urządzenie musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP • Urządzenie musi umożliwiać rozpoznawanie użytkowników oraz ich uwierzytelnianie. • Urządzenie musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: Active Directory, LDAP, Radius, oraz wewnętrznej bazy użytkowników. • Urządzenie musi umożliwiać transparentne uwierzytelnianie użytkowników przez Active Directory. • Urządzenie musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z Microsoft Terminal Services i CitrixXenApp • Urządzenie nie może ograniczać ilości hostów, adresów IP czy użytkowników w sieci wewnętrznej. • Urządzenie musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji • Urządzenie musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen. • Urządzenie musi obsługiwać mechanizmy Protocol Anomaly Detection (PAD) dla najpopularniejszych protokołów. • Urządzenie musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, H.323, SIP, IMAP • Urządzenie musi zapewniać ochronę z wykorzystaniem mechanizmów IPS • Urządzenie musi zapewniać ochronę antywirusową dla obsługiwanych protokołów • Urządzenie musi zapewniać możliwość filtrowania URL • Urządzenie musi zapewniać inspekcję ruchu szyfrowanego HTTPS • Urządzenie musi zapewniać ochronę przed niechcianą pocztą (AntySPAM) • Urządzenie musi mieć możliwość filtrowania treści według typu MIME • Urządzenie musi umożliwiać sterowanie przepustowością w oparciu o następujące parametry: użytkownik, grupa, protokół, polisa, interfejs sieciowy, adres IP, sieć VLAN, aplikacja i kategoria aplikacji • Urządzenie musi udostępniać mechanizmy limitowania dostępu do sieci użytkownikom w oparciu o kwoty czasowe lub transferu danych. • Urządzenie musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site • Urządzenie musi posiadać minimum następujące certyfikaty: ICSA Firewall, FIPS 140-2, Common Criteria EAL4+	

		• Urządzenie musi zapewnić obsługę na poziomie minimalnym: ➢ 40 Gbps dla pracy w trybie firewall, ➢ 13 Gbps dla pracy w trybie IPS, ➢ 8 Gbps dla pracy w trybie UTM full scan (z włączonymi mechanizmami AV and IPS) • Urządzenie musi obsługiwać 7 500 000 jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną 160 0000 nowych połączeń na sekundę • Ilość obsługiwanych sieci VLAN: min 1000 • Minimalna ilość zainstalowanych portów w jednym urządzeniu: ➢ portów 10/100/1000 RJ-45 Base-T: minimum 8 szt. ➢ ilość portów 10Gbps SFP+: minimum 4 szt. ➢ min. 4 szt. modułów 10Gbps SFP+ - zamawiający dopuszcza zamienniki • Urządzenie musi obsługiwać połączenia VPN IPSec typu site-ot-site. • Urządzenie musi w zakresie IPSec site-to-site VPN współpracować z rozwiązaniami innych producentów • Rozwiązanie musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit • Rozwiązanie musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, 3rd Party Cert. • Wsparcie dla Dead Peer Detection (DPD) • Urządzenie musi obsługiwać IKEv1 i IKEv2 • Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego) z podtrzymaniem zestawionych połączeń TCP • Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu • Urządzenie musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP. • Oprogramowanie klienta SSL VPN musi być dostępne dla platform: Windows 7, 8 i 10, MacOS, iOS i Android • Musi być możliwość pobrania klienta SSL bezpośrednio z urządzenia • Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu • Urządzenie ma posiadać certyfikat ICSA IPSec VPN • Przepustowość IPSec VPN (UDP 1518) nie mniejsza niż 10 Gbps • Obsługa nie mniej niż: 5000 tuneli IPSec site-to-site • Obsługa nie mniej niż: 10 000 tuneli client-to-site • Urządzenie musi umożliwiać filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji • Funkcjonalność filtrowania zawartości musi dawać możliwość filtrowania stron według kategorii • Rozwiązanie musi pozwalać na tworzenie białych list wyjątków dla filtrowania zawartości • Funkcja musi filtrować treści w wielu językach, w tym w języku polskim • Filtrowanie musi obsługiwać również protokół HTTPS • Urządzenie musi umożliwiać wyłączenie inspekcji HTTPS dla wybranych kategorii stron www • System kategoryzacji stron musi posiadać kategorie: Command&control, Proxy avoidance, Botnets, Malicious sites, Phishing, Spyware lub równoważnych • System kontroli aplikacyjnej musi rozpoznawać aplikacje oraz kategorie aplikacji	

		• Aplikacje muszą być rozpoznawane w oparciu o analizę ruchu a nie przez porty i protokoły • Ilość rozpoznawanych aplikacji nie mniejsza niż 1800 • W ramach konkretnej aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe) • Kontrola aplikacyjna musi rozpoznawać co najmniej aplikacje: Tor, CryptoAdmin, Skype, Facebook, MS Office 365, Gadu-gadu, Twitter • Automatyczna aktualizacja plików sygnatur antywirusowych • Antywirus musi mieć możliwość przeprowadzania kwarantanny e-mail. • Rozwiązanie musi mieć możliwość tworzenia wyjątków w białej liście, aby umożliwić nieblokowany dostęp do poczty z określonych domen • Wykrywanie i blokowanie spyware'u • Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji • Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S • System musi zapewniać możliwość zablokowania uruchomienia ransomware na stacjach roboczych i serwerach. Jeśli urządzenie wymaga licencji, zamawiający wymaga dostarczenia co najmniej **150 licencji.** • Przepustowość AV w urządzeniu nie mniejsza niż 9,0 Gbps • Antyspam musi zapewnić możliwość kwarantanny e-mail • Antyspam musi posiadać zintegrowaną antywirusową analizę spamu • Rozwiązanie musi umożliwić blokowanie spamu w wielu językach w tym w języku polskim • Automatyczna aktualizacja sygnatur IPS • IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy • Automatyczne blokowanie znanych źródeł ataków • System musi pozwalać na blokowanie ataków typu DoS i DDoS • Przepustowość IPS (full scan) w urządzeniu nie mniejsza niż 2 Gbps • System musi zapewniać ochronę przed nieznanym złośliwym oprogramowaniem, na zasadzie analizy behawioralnej (sandbox). • Analizie muszą podlegać pliki ściągane przez http(s) i przesyłane pocztą elektroniczną. • System musi zapewniać ogólne oszacowanie poziomu ryzyka dla analizowanych plików oraz udostępniać szczegółowe informacje o wykrytych działaniach niebezpiecznych. • System musi mieć możliwość blokowania poczty zawierającej podejrzane załączniki do czasu zakończenia ich analizy • Administracja urządzenia musi być możliwe poprzez graficzny interfejs zarządzania w czasie rzeczywistym. Nie powinno być konieczne jakiekolwiek dodatkowe oprogramowanie służące do konfiguracji rozwiązania. • Urządzenie musi umożliwiać zarządzanie za pomocą linii poleceń poprzez port szeregowy lub poprzez SSH. • Urządzenie musi umożliwiać zarządzanie za pomocą wbudowanego interfejsu www. • Interfejs WWW do zarządzania urządzeniem musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach. • Urządzenie może być zarządzane jednocześnie z wielu platform przez różnych administratorów.	

		• Rozwiązanie musi umożliwiać wysyłanie alarmów przez SNMP lub e-mail. • Rozwiązanie musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online • System musi posiadać metodę porównywania różnych wersji konfiguracji. • Obsługa różnych ról administratorów. • Umożliwia monitorowanie logów ruchu w czasie rzeczywistym. • Urządzenie musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi. • Rozwiązanie musi umożliwiać zbieranie i przechowywanie dzienników i raportów. • Rozwiązanie musi umożliwiać przesyłanie logów do co najmniej 2 serwerów dziennika (log server). • Serwer logów musi być osobny urządzeniem lub maszyną wirtualną. W przypadku maszyny wirtualnej musi być zapewniona współpraca z wirtualizatorem VMware lub Microsoft Hyper-V. • Rozwiązanie musi zbierać logi przynajmniej z 20 urządzeń tego samego producenta • Dzienniki transmisji muszą być szyfrowane. • Rozwiązanie musi zapewniać narzędzie graficznej analizy logów. • Rozwiązanie musi udostępniać narzędzie analizy całości ruchu • Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa • Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów • Serwer logów musi umożliwiać zapis do wbudowanej bazy danych lub do zewnętrznej bazy danych. • Rozwiązanie musi umożliwiać stały dostęp do logów w celu analizy i generowania raportów. • Rozwiązanie musi posiadać minimum 90 predefiniowanych typów raportów. • Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie • Urządzenie musi mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV. • System musi być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania tych sprawozdań pocztą e-mail. • Musi być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości. • System raportowania musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów i dzienników. • System musi wspierać automatyczne wysyłanie wszystkich typów raportów pocztą elektroniczną. • Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom. • System musi umożliwiać pseudoanonimizację użytkowników z prawem do deanonimizacji tylko dla wybranych administratorów. • System powinien zapewniać wizualizację, opisującą w trybie graficznym stan przepustowości systemu. • System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych. • Okres wsparcia technicznego – dotyczy urządzenia minimum 60 miesięcy.	

		• Urządzenie musi być dostarczone ze wszystkimi licencjami/subskrypcjami umożliwiającymi uzyskanie funkcjonalności wymienionymi w niniejszym OPZ. Długość trwania licencji/subskrypcji nie może być krótsza niż okres wsparcia technicznego. • Możliwość zgłaszania incydentów za pomocą e-mail, portalu - 24 godziny na dobę 7 dni w tygodniu • Zamawiający wymaga by wymiana urządzenia w przypadku zdiagnozowania awarii uniemożliwiającej funkcjonowanie, następowała na następny dzień roboczy od zdiagnozowania awarii (advaced hardware replacement NBD)	

Parametry punktowane

Lp.	Parametry punktowane	
Parametry techniczne – Router z funkcjami zabezpieczającymi		
1	• Wysokość pojedynczego urządzenia maksimum 1U • Każde urządzenie klastra posiada możliwość przyszłej rozbudowy o minimum dodatkowe cztery porty 10Gb SFP+ bez konieczności deinstalacji lub wymiany portów dostarczanych w niniejszym postępowaniu. Jeśli urządzenie nie posiada możliwości rozbudowy, Wykonawca musi zaoferować rozwiązanie wyposażone w minimum osiem portów 10Gb SFP+. • Serwer logów umożliwia zapis do wbudowanej bazy danych lub do zewnętrznej bazy danych. • Urządzenie posiada rozwiązanie Antyspam oparte na technologii RPD - Recurrent Pattern Detection. • Urządzenie umożliwia zdefiniowanie 4 i więcej stref bezpieczeństwa. • Rozwiązanie umożliwia edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji z wykorzystaniem dodatkowego oprogramowania producenta. • System posiada możliwość stworzenia mapy sieci wewnętrznej zawierającej szczegółowe dane urządzenia (MAC, IP, System operacyjny, otwarte porty).	**TAK** – 20 punktów **NIE** – 0 punktów
2	Urządzenie posiada system blokowania i odpowiedzi na zaawansowane zagrożenia typu malware i ransomware o parametrach: • posiada agentów dedykowanych dla systemów operacyjnych co najmniej Windows 7, 8, 8.1, 10, Windows Server 2008, 2012, 2016, Linux RedHat/CentOS, Mac OS 10.x, • dostarczone z licencją na wsparcie co najmniej 250 hostów (stacji roboczych i serwerów), • system posiada możliwość prowadzenia analizy heurystycznej i behawioralnej pod katem zagrożeń typu malware i ransomware, bezpośrednio na hostach i w trybie ciągłym wysyła wyniki analizy do systemu centralnego w celu przeprowadzenia oceny zagrożeń dzięki korelacji i scoringu zagrożeń, • system posiada mechanizm automatycznej odpowiedzi na wykryte zagrożenie typu malware i ransomware, poprzez minimum takie działania jak, kwarantanna plików, zabijanie procesów (ang. kill) i usuwanie wpisów w rejestrach, • system pozwala na konfigurowalne powiadamianie poprzez e-mail minimum o wykrytych krytycznych zdarzeniach, incydentach, oraz akcjach podjętych aby im zapobiec które miały miejsce w sieci i na hostach,	**TAK** – 20 punktów **NIE** – 0 punktów