Załącznik nr 3 do zapytania ofertowego nr NI.2810.16.2021-ZOF

Marek Staszewski

Elektronicznie podpisany przez Marek Staszewski
Data: 2021.03.11 14:09:41 +01'00'

FORMULARZ OFERTY

Pełna nazwa oferenta:	

Adres oferenta:	Ulica:	Nr:
	Kod pocztowy:	Miejscowość:
	Nr telefonu:	Fax:
	e-mail:	
REGON:	NIP:	
Bank:	Nr konta:	
Nr wpisu do KRS / nazwa w CEiDG		
Wykonawca należy do sektora **MŚP (małych i średnich przedsiębiorstw)** ☐ TAK ☐ NIE (zaznaczyć właściwe)		

1. Opis przedmiotu zamówienia – parametry wymagane

PARAMETRY WYMAGANE	PARAMETRY OFEROWANE (UZUPEŁNIĆ)
WYMAGANIA OGÓLNE	
Praca w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN	
Budowa minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji	
Dedykowanie co najmniej 3 administratorów do poszczególnych instancji systemu	
Wsparcie IPv4 oraz IPv6 w zakresie: • Firewall • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego	
REDUNDANCJA, MONITORING I WYKRYWANIE AWARII	
W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS ma możliwość łączenia w klaster Active-Active lub Active-Passive	
W obu trybach Active-Active lub Active-Passive istnieje funkcja synchronizacji sesji firewall	
System dostarczony jest w postaci redundantnej	
Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych	
Monitoring stanu realizowanych połączeń VPN	
Agregacja linków statyczną oraz w oparciu o protokół LACP	
Tworzenie interfejsów redundantnych	

INTERFEJSY, DYSK, ZASILANIE	
18 portów Gigabit Ethernet RJ-45	
8 gniazd SFP 1 Gbps	
4 gniazdami SFP+ 10 Gbps (do zestawu muszą być dołączone moduły światłowodowe/wkładki 10GbE SFP+)	
Wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB	
Możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q	
Zasilanie AC	
PARAMETRY WYDAJNOŚCIOWE	
Obsługa przez Firewall'a nie mniej niż 3 mln. jednoczesnych połączeń oraz 250 tys. nowych połączeń na sekundę	
Przepustowość Stateful Firewall: nie mniej niż 27 Gbps dla pakietów 512 B	
Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 12 Gbps	
Wydajność szyfrowania IPSec VPN nie mniej niż 12 Gbps	
Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps	
Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps	
Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps	
FUNKCJE SYSTEMU BEZPIECZEŃSTWA (MOGĄ 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	

Zarządzanie pasmem (QoS, Traffic shaping)	
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	
Analiza ruchu szyfrowanego protokołem SSL	
Analiza ruchu szyfrowanego protokołem SSH	
POLITYKI, FIREWALL	
Polityka Firewall uwzględnia adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń	
Translacja adresów NAT: źródłowego i docelowego	
Translację PAT	
Translacja jeden do jeden oraz jeden do wielu	
Dedykowany ALG (Application Level Gateway) dla protokołu SIP	
Tworzenie wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN	
Element systemu realizujący funkcję Firewall integruje 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 • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware vCenter (ESXi).	
POŁĄCZENIA VPN	
System umożliwia konfigurację połączeń typu IPSec VPN	
W zakresie IPSec VPN system zapewnia:	
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 Diffie-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	
Wybór 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 umożliwia konfigurację połączeń typu SSL VPN	
W zakresie SSL VPN system zapewnia:	
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	
Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN	
ROUTING I OBSŁUGA ŁĄCZY WAN	
Routing statyczny	
Policy Based Routingu	
Protokoły dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM	
ZARZĄDZANIE PASMEM	
Zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu	
Określanie pasma dla poszczególnych aplikacji	
Zarządzanie pasmem dla wybranych kategorii URL	
OCHRONA PRZED MALWARE	
Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).	
Skanowanie archiwów, w tym co najmniej: zip, RAR	
System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android)	
System współpracuje 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)	

System umożliwia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików	
OCHRONA PRZED ATAKAMI	
Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych	
Ochrona 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 ma możliwość definiowania własnych wyjątków oraz własnych sygnatur	
System zapewnia 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	
KONTROLA APLIKACJI	
Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP	
Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora	
Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików	
Baza zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P	
Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur	
KONTROLA WWW	
Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne	
W ramach filtra www dostępne są kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy	
Filtr WWW dostarcza kategorii stron zabronionych prawem: Hazard	

Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL	
Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo	
Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania	
W ramach systemu istnieje możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji	
UWIERZYTELNIANIE UŻYTKOWNIKÓW W RAMACH SESJI	
System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu	
System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP	
System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych	
Możliwość zastosowania uwierzytelniania dwu-składnikowego	
Budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API	
ZARZĄDZANIE	
Elementy systemu bezpieczeństwa mają możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH	
Możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania	
Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów	
Włączenie mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego	
Współpraca z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3	
Przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow	
Zarządzanie przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację	

Element systemu pełniący funkcję Firewal posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall	
Element systemu realizujący funkcję firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone	
LOGOWANIE	
Elementy systemu bezpieczeństwa realizują 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	
W ramach logowania system pełniący funkcję Firewall zapewnia przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu	
Jednoczesne wysyłania logów do wielu serwerów logowania	
Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu	
Logowania do serwera SYSLOG	
CERTYFIKATY	
ICSA lub EAL4 dla funkcji Firewall	
SERWISY I LICENCJE	
Licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.	
GWARANCJA ORAZ WSPARCIE	
Serwis gwarancyjny producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości	
Dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	

ROZSZERZONE WSPARCIE SERWISOWE AHB/SOS	
Rozszerzone wsparcie techniczne gwarantujące udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu na następny dzień roboczy od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy Oferent winien przedłożyć dokumenty: • Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego.	
DOKUMENTY	
Dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.)	
Dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania	
Oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań	
WDROŻENIE / INSTALACJA	
Usługa wdrożenia urządzeń w sieci Zamawiającego	
Migracja konfiguracji z posiadanych urządzeń oraz wdrożenia segmentacji sieci na dostarczonych urządzeniach	
Instalacja musi zostać wykonana przez inżyniera posiadającego certyfikat producenta w siedzibie Zamawiającego.	
Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu	
Pełna konfiguracja urządzenia przez certyfikowanego inżyniera zgodnie z wymaganiami użytkownika, najlepszymi praktykami i doświadczeniem inżynierów na podstawie szablonów i przeprowadzonych konsultacji z uwzględnieniem poprzedniej konfiguracji firewall`a	
Aktualizacja oprogramowania do najnowszej wersji	
Poprawa polityk firewall`a	

Podniesienie poziomu bezpieczeństwa	
Testy poprawności działania urządzenia	
WSPARCIE TECHNICZNE WYKONAWCY	
60 miesięcy - telefon, e-mail, system helpdesk, połączenia zdalne	
usługi wsparcia w konfiguracji urządzeń, rekonfiguracji oraz pomocy w sytuacjach, które wymagają zmian sieci lub dotyczą konfiguracji bezpieczeństwa sieciowego	

Oferowane urządzenia muszą być **fabrycznie nowe, rok produkcji 2020 lub 2021**.

2. CENA i OŚWIADCZENIA WYKONAWCY

1. Składamy ofertę na wykonanie zamówienia zgodnie z zakresem opisanym w niniejszym formularzu za **cenę:**

l.p.	**Opis**	**Ilość**	**Cena jednostkowa netto [PLN]**	**VAT (%)**	**wartość netto [PLN]**	**wartość brutto [PLN]**
1.	**Urządzenie UTM (klaster)** Typ urządzenia (producent, model): …….. Rok produkcji: …….	**2**				
				RAZEM:		

Wartość oferty (cena łączna) słownie
netto: ……..
brutto: …….

2. Uważamy się za związanych niniejszą ofertą przez okres 30 dni od upływu terminu składania ofert.
3. Oświadczamy, że akceptujemy przedstawiony przez Zamawiającego projekt umowy, nie wnosimy do niego zastrzeżeń i w przypadku wyboru naszej oferty zobowiązujemy się do podpisania umowy na zawartych w nim warunkach.
4. Zobowiązujemy się dostarczyć przedmiot zamówienia w terminie 14 dni od daty zawarcia umowy
5. Dane kontaktowe osoby upoważnionej do kontaktu z Zamawiającym w sprawach związanych z postępowaniem
   Imię i nazwisko_____
   Nr telefonu_____
   e-mail_____

6. W przypadku wyboru naszej oferty, umowę podpisze:
   Imię i nazwisko_____

_____
miejscowość, data (podpis oferenta)