OPZ - Wymagane parametry techniczne – opis wymagań minimum

Firewall typ 1.2

Ilość: 6 szt.

Identyfikator produktu Zamawiającego: T051201-012 (T-04-06-01-02)

Lp.	Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne	Spełnienie Parametrów technicznych oferowanego urządzenia
1	2	3	4
1	Model	W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia.	…… **/Podać producenta urządzenia/** …… **/Podać model, symbol/**
2	Architektura systemu	Obsługa sprzętowa dla minimum następujących funkcji ochronnych: • firewall klasy : ”Statefull Inspection” • system VPN z obsługą IPSec i SSL, • zapobieganie wyciekowi danych ~~poufnych (DLP).~~ • system antywirusowy dla protokołów SMTP, POP3, http, FTP, IMAP lub POP3S, • ochronę przed atakami bazującą na systemach prewencji i detekcji (IPS oraz IDS), • kontrolę treści – Web Filter • kontrolę zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP lub POP3S • kontrolę pasma oraz ruchu [QoS i Traffic shaping] • kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM oraz P2P lub na podstawie sygnatur kontekstowych rozpoznających typ aplikacji) • SSL proxy z możliwością pełniej analizy szyfrowanej komunikacji dla wybranych protokołów	…… /Wpisać: spełnia lub nie spełnia/

		Funkcje ochronne realizowane sprzętowo przy użyciu specjalizowanych układów scalonych ASIC lub system operacyjny zoptymalizowany do wykonywania tych funkcji na platformach bez układów ASIC.	…… /Wpisać: spełnia lub nie spełnia/
		W celu zapewnienia wysokiej niezawodności system operacyjny oraz inne dane konfiguracyjne i tworzone w trakcie pracy muszą być zapisywane ~~wyłącznie~~ na urządzenia pamięci typu FLASH lub na dysku twardym urządzenia.	…… /Wpisać: spełnia lub nie spełnia/
		Wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny muszą pochodzić od jednego producenta lub producent rozwiązania świadczy wsparcie dla wszystkich tych modułów, które nie pochodzą od producenta rozwiązania – pochodzą od różnych dostawców funkcji bezpieczeństwa.	…… /Wpisać: spełnia lub nie spełnia/
		Warunki licencjonowania wszystkich funkcji ochronnych bez limitu chronionych zasobów (licencja na urządzenie).	…… /Wpisać: spełnia lub nie spełnia/
		Licencje na funkcje ochronne: firewall, ~~DLP~~ oraz systemu VPN bez limitu czasowego na działanie ale z dopuszczalnym limitem czasowym na aktualizacje systemów (koniec aktualizacji wraz z końcem licencji aktualizacyjnej na urządzenie).	…… /Wpisać: spełnia lub nie spełnia/
		Z urządzeniem dostarczone niezbędne oprogramowanie i licencje na minimum: • system firewall, • system VPN, • ~~system DLP,~~ • system filtrowania treści (Web Filtering) • system antywirusowy, • system prewencji przed włamaniami IPS • system detekcji ataków IDS • system antyspamowy, • system kontroli aplikacji, • system kontroli ruchu sieciowego przez okres minimum 24 miesiące	…… /Wpisać: spełnia lub nie spełnia/
3	System operacyjny	Dedykowany system operacyjny czasu rzeczywistego. System musi pochodzić od producenta urządzenia. Nie dopuszcza się stosowania komercyjnych i niekomercyjnych (licencja GPL) systemów operacyjnych ogólnego przeznaczenia.	…… /Wpisać: spełnia lub nie spełnia/

4	Ilość/rodzaj portów	• minimum 4 porty 10/100/1000 Base-TX Ethernet w tym minimum 2 porty WAN, minimum 1 port DMZ, minimum 1 porty LAN, • minimum 1 port typu SFP do obsługi modułów światłowodowych Gigabit Ethernet • port administracyjny do bezpośredniego podłączenia konsoli, • port USB do podłączenia zewnętrznych nośników	…… /Wpisać: spełnia lub nie spełnia/
5	Zasada działania (tryby)	Urządzenie powinno obsługiwać następujące tryby pracy: • jako router z obsługą NAT pracujący w III warstwie ISO-OSI, • jako most z obsługą transparent bridge pracujący w II warstwie ISO-OSI.	…… /Wpisać: spełnia lub nie spełnia/
6	Funkcje firewall	~~1. Możliwość definiowania bez dodatkowych licencji minimum 5 wirtualnych firewalli posiadających:~~ ~~• indywidualne tabele routingu,~~ ~~• polityki bezpieczeństwa,~~ ~~• dostęp administracyjny.~~ Pozostała numeracja nie ulega zmianie. 2. Obsługa Policy Routingu w oparciu o: • typ protokołu, • numer portu TCP/UDP • interfejs, • adres IP źródłowy, • adres IP docelowy. 3. Obsługa routingu statycznego. 4. Obsługa protokołów routingu dynamicznego: • RIPv2, • OSPF, • BGP-4. (dopuszcza się obsługę innych protokołów routingu) 5. Statyczna i dynamiczna translacja adresów (NAT). 6. Przepustowość w trybie ~~statefull min. 300 Mb/s dla pakietów 512B~~ firewall min.10 Gbps niezależnie od wielkości pakietów, 7. Liczba jednocześnie działających reguł minimum 4000,	…… /Wpisać: spełnia lub nie spełnia/

7	Funkcje IDS/IPS lub w zakresie ppkt. 2. na podstawie MIME Type plików.	1. Wykrywanie i blokowanie technik i ataków: • SYN Attack, • ICMP Flood, • IP Spoofing, • UDP Flood, • Port Scan 2. Wykrywanie i blokowanie niebezpiecznych komponentów: • Java, • ActiveX. 3. Ochronę sieci VPN przed atakami Replay Attack 4. Limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. 5. Aktualizacja bazy sygnatur może się odbywać ręcznie lub automatycznie 6. Wykrywanie połączeń peer-to peer 7. Dziennik zdarzeń (logging)z możliwością zapisania w pliku,	…… /Wpisać: spełnia lub nie spełnia/
8	Połączenia VPN	1. Tworzenie połączeń w topologii Site-to-site oraz Client-to-site 2. Dostawca musi udostępniać oprogramowanie klienta VPN dla Windows 7/ 8/ 10 realizujące funkcje: • firewall, • antywirus, • web filtering, • antyspam lub zapewnić na urządzeniu możliwość tunelowania ruchu umożliwiającego wykonanie takiej analizy na urządzeniu. 3. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności 4. Obsługa VPN z wykorzystaniem mechanizmów: IPSec i SSL 5. Liczba dedykowanych tuneli minimum 50	…… /Wpisać: spełnia lub nie spełnia/
9	Uwierzytelnianie użytkowników	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: • haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia • haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych. • haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP • Rozwiązanie powinno umożliwiać budowę logowania Single Sign On w środowisku Active Directory bez dodatkowych opłat licencyjnych.	…… /Wpisać: spełnia lub nie spełnia/

10	Funkcjonalność zapewniająca niezawodność	1. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. 2. Urządzenia połączone w klaster typu Active-Active lub Active-Passive. 3. Dostarczone wszystkie niezbędne kable przyłączeniowe i inne akcesoria pozwalające na utworzenie klastra. 4. Posiadanie nieulotnej pamięci wewnętrznej do zapisu zdarzeń typu log o wielkości minimum 250GB.	…… /Wpisać: spełnia lub nie spełnia/
11	Obudowa	Obudowa ma posiadać wymiary i odpowiednie uchwyty i śruby do zamontowania w szafie 19”.	…… /Wpisać: spełnia lub nie spełnia/
12	Wydajność	1. Obsługa nie mniej niż ~~2~~ 1 milion~~y~~ jednoczesnych sesji TCP 2. Obsługa minimum 20 tysięcy nowych sesji TCP na sekundę. 3. Przepustowość dla ruchu nieszyfrowanego minimum 900 Mb/s 4. Przepustowość dla IPsec VPN minimum ~~300 Mb/s (pakiety 512 bajty)~~ 2Gbps niezależnie od wielkości pakietów. ~~5. Opóźnienie Firewalla dla pakietów UDP o dł. 64 bajty nie więcej niż 40 µs~~ 6. Przepustowość systemu IPS minimum 900 Mb/s, 7. Przepustowość systemu Antywirusowego w trybie on-line (FlowBase) minimum 600Mb/s	…… /Wpisać: spełnia lub nie spełnia/
13	Zasilanie	Zasilanie z sieci 220-240V/50Hz.	…… /Wpisać: spełnia lub nie spełnia/
14	Konfiguracja i zarządzanie	1. Możliwość konfiguracji poprzez terminal i linię komend (CLI) oraz konsolę graficzną (GUI). 2. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. 3. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. 4. Administratorzy muszą być uwierzytelniani za pomocą haseł statycznych lub haseł dynamicznych (RADIUS). 5. System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB.	…… /Wpisać: spełnia lub nie spełnia/

15	Zarządzanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem centralnego zarządzania dostępnym w ofercie producenta oferowanych urządzeń lub w formie maszyny wirtualnej, który umożliwia: • Zarządzanie wersjami firmware'u na urządzeniach oraz zdalne uaktualnienia, • Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia lub oferowane urządzenie ma funkcje automatycznej aktualizacji baz sygnatur, • Monitorowanie w czasie rzeczywistym obciążenia nu urządzeń, • Zapis i zdalne wykonywanie skryptów na urządzeniach, • Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń.	…… /Wpisać: spełnia lub nie spełnia/
16	Certyfikaty	Urządzenie musi posiadać następujące certyfikaty: UTM NSS Approved, EAL4+, ICSA Labs dla funkcji: Firewall, IPSec, SSL, Network IPS, Antywirus lub certyfikaty EAL4+ dla funkcji firewall oraz EU Restricted oraz NATO Restricted.	…… /Wpisać: spełnia lub nie spełnia/
17	Aktualizacje oraz serwis	Wykonawca wraz z urządzeniami dostarczy wszelkie licencje aktywacyjne dla funkcji bezpieczeństwa oraz subskrypcję na aktualizację baz sygnatur systemu IPS/IDS, baz antywirusowych i antyspamowych oraz dostępu do systemu filtrowania treści na okres 24 miesięcy.	…… /Wpisać: spełnia lub nie spełnia/
		Minimum 24 miesiące gwarancji. (warunki gwarancji zgodnie z zapisami we wzorze umowy stanowiącym załącznik 8 do SIWZ)	…… /Wpisać: spełnia lub nie spełnia/ …… **/Podać ilość miesięcy oferowanej gwarancji/**
18	Dodatkowe wymagania:	Do każdego urządzenia należy dołączyć: • Komplet kabli zasilających. • Dokumentację.	…… /Wpisać: spełnia lub nie spełnia/
19	Wdrożenie i szkolenie	Wykonawca zapewni instalację klastra i jego konfigurację oraz wstępne przeszkolenie administratorów podczas instalacji i konfiguracji Sprzętu. Wdrożenia dokona certyfikowany inżynier (certyfikat poświadczający zdanie egzaminów i znajomość konfiguracji dostarczonych urządzeń na poziomie min. II producenta oferowanego rozwiązania)	…… /Wpisać: spełnia lub nie spełnia/

20	Certyfikaty i dokumenty	• Urządzenia wyprodukowane są przez producenta, u którego wdrożono normę PN-EN ISO 9001 lub równoważną, w zakresie co najmniej produkcji lub projektowania lub rozwoju urządzeń lub systemów lub rozwiązań informatycznych. • Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 14001 lub równoważną. • Oferowane urządzenia posiadają deklarację zgodności CE	…… /wpisać spełnia lub nie spełnia/

Uwaga:

Brak wypełnienia wszystkich pozycji „W*ymaganych parametrów technicznych – opis wymagań minimum*" w kolumnie „***Spełnienie parametrów technicznych oferowanego urządzenia***" będzie uważane za niespełnienie warunków minimalnych przez oferowane urządzenie i będzie skutkowało odrzuceniem oferty.

data: .....

.....
podpis/y/ osoby/osób upoważnionej/nych
do występowania w imieniu Wykonawcy
oraz pieczątka/ki imienna/e