Załącznik nr 1 do Formularza Ofertowego

Specyfikacja techniczna oferowanego sprzętu

Zapora ogniowa Router-Firewall z kontrolerem sieci bezprzewodowej WiFi – wymagane podanie konkretnych parametrów i informacji na temat oferowanego urządzenia.

Specyfikacja techniczna (producent, nazwa, typ):

.....

Wymagane minimalne parametry techniczne urządzenia	Parametry oferowanego urządzenia
1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.	
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.	
3. Monitoring stanu realizowanych połączeń VPN.	
4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.	
5. System realizujący funkcję Firewall powinien dysponować minimum - 7 portami Ethernet 10/100/1000 Base-TX.	
6. System powinien umożliwiać zdefiniowanie co najmniej 250 interfejsów wirtualnych - definiowanych jako VLAN w oparciu o standard 802.1Q.	
7. W zakresie Firewall obsługa nie mniej niż - 1,5 mln jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę.	
8. Przepustowość Firewall: nie mniej niż - 2 Gbps.	
9. Wydajność szyfrowania VPN IPSec: nie mniej niż 180 Mbps.	
10. System powinien 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 platformy sprzętowej lub programowej.	
11. System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń.	
12. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:	
☐ Kontrola dostępu - zapora ogniowa klasy Stateful Inspection	
☐ Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS	

Załącznik nr 1 do Formularza Ofertowego

⍰ Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN	
⍰ Ochrona przed atakami - Intrusion Prevention System	
⍰ Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.	
⍰ Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP	
⍰ Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma	
⍰ Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów)	
⍰ Możliwość analizy ruchu szyfrowanego protokołem SSL	
⍰ Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)	
13. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 700 Mbps,	
14. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 160 Mbps,	
15. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż:	
⍰ Tworzenie połączeń w topologii Site-to-site oraz Client-to-site	
⍰ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności	
⍰ Praca w topologii Hub and Spoke oraz Mesh	
⍰ Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF	
⍰ Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth.	
16. W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.	
17. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.	
18. Translacja adresów NAT adresu źródłowego i docelowego.	
19. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.	
20. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.	

Załącznik nr 1 do Formularza Ofertowego

21. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR.	
22. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS.	
23. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.	
24. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.	
25. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.	
26. System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż:	
☐ 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	
☐ Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory	
27. 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: SSL VPN, IPSec VPN	
28. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	
29. Serwisy i licencje: W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 2 lat.	

Załącznik nr 1 do Formularza Ofertowego

30. Gwarancja oraz wsparcie: System powinien być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku, gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, Oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej Całość rozwiązania musi być objęta 2-letnim wsparciem producenta FW/ kontroler sieci WiFi/ punkty dostępowe WiFi.	

Przełącznik sieciowy 8 – portowy – wymagane podanie konkretnych parametrów i informacji na temat oferowanego urządzenia.
Specyfikacja techniczna (producent, nazwa, typ):
.....

Wymagane minimalne parametry techniczne urządzenia	Parametry oferowanego urządzenia
1. Parametry fizyczne platformy:	
• wymiary urządzenia powinny pozwalać na montaż w szafie RACK 19", obudowa nie powinna być wyższa niż 1U	
• Zasilanie 230V	
2. Interfejsy sieciowe – wymagania minimalne:	
• 8 portów GE, RJ-45 z zasilaniem 802.3af/at	
• 2 porty GE SFP	
3. Parametry wydajnościowe:	
• przepustowość urządzenia - min. 20 Gbps	
• możliwość zapamiętania co najmniej 16 000 adresów MAC	
• Opóźnienie - poniżej 2 mikrosekund	
4. Wymagane funkcje:	
• możliwość automatycznej negocjacji prędkości i duplexu dla połączeń	
• obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree)	
• możliwość agregacji portów zgodna z 802.3ad	
• obsługa co najmniej 4000 VLANów, zgodna z 802.1Q	
• możliwość wykonywania routingu statycznego	
• port-mirroring	
• Kontrola dostępu na poziomie portu w oparciu o standard 802.1x, możliwość uwierzytelniania w oparciu o bazę Radius	

Załącznik nr 1 do Formularza Ofertowego

• zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS, SNMP w wersjach 1-3, SNTP, LLDP (w trybie odbioru)	
• możliwość zarządzania przez interfejs graficzny i tekstowy	
• możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI	
• **integracja z systemem bezpieczeństwa (NGFW, UTM), opisanym w pkt. a powyżej, pochodzącym od tego samego producenta, w zakresie co najmniej:**	
- możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników,	
- obsługa białych i czarnych list MAC,	
- Stateful Firewall, umożliwiający kontrolę dostępu pomiędzy segmentami sieci,	
- routing statyczny i dynamiczny, co najmniej OSPF.	
5. Gwarancja: urządzenia powinny być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku, gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej. Całość rozwiązania musi być objęta 2-letnim wsparciem producenta FW/ kontroler sieci WiFi/ przełącznik sieciowy i punkty dostępowe WiFi.	

Punkt dostępowy sieci bezprzewodowej WiFi – wymagane podanie konkretnych parametrów i informacji na temat oferowanego urządzenia.

Specyfikacja techniczna (producent, nazwa, typ): .....

Wymagane minimalne parametry techniczne urządzenia		**Parametry oferowanego urządzenia**
Tryb pracy	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.	
Obudowa	Kompaktowa obudowa z tworzywa sztucznego umożliwiającą montaż na suficie lub ścianie wewnątrz budynku.	

Załącznik nr 1 do Formularza Ofertowego

Moduł radiowy	Musi być wyposażony w moduł radiowy pracujący odpowiednio w pasmach: 5 GHz a/n lub 2,4 GHz b/g/n. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 7 SSID Przepustowość radia: 300 Mbps Mechanizmy kolejkowania dla różnych klas ruchu: dane, Voice, video Mechanizmy ochrony przed atakami na sieć radiową Wymagana moc nadawania dla częstotliwości 2,4 GHz - min 18 dBm Mechanizmy uwierzytelniania 802.1x, w tym obsługa EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, Możliwość tunelowania całej komunikacji do kontrolera sieci bezprzewodowych jak również funkcja bridge'owania ruchu z poszczególnych SSID do VLAN.	
Anteny	Minimum 2 wbudowane anteny	
Interfejsy	Interfejs sieciowy w standardzie 10/100/1000 Base-TX	
Integracja	W celu zapewnienia spójności polityk bezpieczeństwa, zarządzanie planowaną strukturą punktów dostępowych WiFi powinno odbywać się z dostarczonych w ramach postępowania zapór ogniowych Firewall.	
Zarządzanie punktem dostępowym	Kontroler powinien oferować środowisko graficzne pozwalające na wykrywanie punktów dostępowych podpinanych do sieci, a następnie na zarządzanie nimi.	
Zasilanie	Możliwość zasilania w standardzie PoE 802.3af	
Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej. Całość rozwiązania musi być objęta 2-letnim wsparciem producenta FW/ kontroler sieci WiFi/ punkty dostępowe WiFi.	