Nr sprawy: **FZ-1/5613/MKO/21/FI** **Katowice, 17.11.2021 r.**

Dotyczy : Wstępnego zapytania ofertowego w celu ustalenia wartości zamówienia

Szanowni Państwo,

Zwracamy się z prośbą o wstępną ofertę na dostawę, wdrożenie oraz serwis Centralnego Systemu Ochrony Sieci.

Centralny System Ochrony Sieci musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa, niezależnie od dostawcy łącza sieciowego. System ten musi składać się co najmniej z klastra urządzeń ochrony sieci. Zamawiający dopuszcza, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. Platformy wirtualne muszą wspierać następujące rodzaje hypervisorów: ESXi v6.5 lub wyższe, XenServer v6.0 lub wyższe, Hyper-V 2008R2 lub wyższe, AWS lub wyższe, Azure, CentOS v6.4 lub wyższe. System ma zapewniać zbieranie i analizę logów. Wszystkie licencje wchodzące w skład systemu muszą być bezterminowe.

Klaster urządzeń ochrony sieci

1. Architektura systemu ochrony:
   - W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym;
   - System musi wspierać IPv4 oraz IPv6 w zakresie min. firewall, ochrony w warstwie aplikacji, protokołów routingu dynamicznego;
   - System ochrony musi być zbudowany przy użyciu minimalnej ilości elementów ruchomych, krytycznych dla jego działania. Dlatego, główne urządzenie ochronne (ang. *gateway*) nie może posiadać twardego dysku, w zamian powinno używać pamięci typu *flash*;
   - Urządzenie powinno być wyposażone w specjalizowane układy sprzętowe typu ASIC (ang. *Application Specific Integrated Circuit*) realizujące podstawowe funkcje ochronne;
   - Wymagane jest, by na wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny, Zamawiający uzyskał licencje bez limitu chronionych urządzeń użytkowników (licencje na urządzenie);
   - System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych;
   - W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – powinna być możliwość łączenia urządzeń w klaster Active-Active lub Active-Passive;
   - W ramach postępowania system musi zostać dostarczony w postaci klastra HA (ang. *High Availability*).
2. Ilość/rodzaj portów i modułów dla pojedynczego urządzenia (Zamawiający wymaga, żeby urządzenia w klastrze były tak samo wyposażone):

- Nie mniej niż 18 portów RJ45 GigabitEthernet 10/100/1000 Base-TX;
- Nie mniej niż 8 portów SFP GigabitEthernet 10/100/1000;
- Nie mniej niż 4 porty SFP+ TenGigabitEthernet 10/100/1000/10000;
- Każdy z portów typu SFP, musi być wyposażony w odpowiedni moduł połączeniowy, w pełni kompatybilny z urządzeniem – specyfikacja w punkcie 'Wyposażenie dodatkowe';
- Każdy z portów typu SFP+, musi być wyposażony w odpowiedni moduł połączeniowy, w pełni kompatybilny z urządzeniem – specyfikacja w punkcie 'Wyposażenie dodatkowe';
- Nie mniej niż 200 interfejsów wirtualnych VLAN w oparciu o standard IEEE802.1q.

3. Wydajność:
   - W zakresie funkcjonalności Firewall obsługa minimum 3 mln jednoczesnych połączeń i minimum 250 tys. nowych połączeń na sekundę;
   - Przepustowość Firewall mierzona przy obsłudze pakietu 512b: minimum 25 Gbps;
   - Wydajność szyfrowania VPN IPSec (z wykorzystaniem algorytmu AES-256): minimum 12 Gbps;
   - Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno po stronie klienta, jak i serwera w ramach modułu IPS) mierzona przy włączonej obsłudze klasy *Stateful Inspection*: minimum 5 Gbps;
   - Wydajność skanowania ruchu z włączoną funkcją Antywirus mierzona przy włączonej obsłudze klasy *Stateful Inspection*: minimum 3 Gbps;
   - Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTP – minimum 4 Gbps.
4. Zapewnienie niezawodności:
   - Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych;
   - Monitoring stanu realizowanych połączeń VPN.
5. Dostępne funkcjonalności:
   - Kontrola dostępu - zapora ogniowa klasy *Stateful Inspection*;
   - Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS;
   - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN;
   - Ochrona przed szkodliwym oprogramowaniem *malware* – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
   - Ochrona przed atakami (ang. *Intrusion Prevention System*);
   - Kontrola pod kątem rozpoznawania witryn internetowych potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, szpiegujących i generujących spam;
   - Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP;
   - Kontrola pasma oraz ruchu (ang. *Quality of Service, Traffic Shaping*) – co najmniej określanie maksymalnej i gwarantowanej wielkości pasma;
   - Kontrola aplikacji – system musi rozpoznawać aplikacje typu: P2P, Botnet, Proxy Avoidance;
   - Możliwość analizy ruchu szyfrowanego protokołem SSL;
   - Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
6. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z dwóch trybów: routera z funkcją NAT lub trybie transparentnym (ang. *bridge*).
7. Polityka bezpieczeństwa:
   - Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i zarządzanie pasmem sieci;
   - W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa (np. DMZ, LAN, WAN);
   - Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN (ang. *Software-Defined Networking*): Amazon Web Services (AWS), Microsoft Azure, Cisco ACI, Google Cloud Platform (GCP), OpenStack, VMware vCenter (ESXi); w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
8. Ochrona przed szkodliwym oprogramowaniem *malware*

- Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021);
- System musi umożliwiać skanowanie archiwów, w tym co najmniej ZIP i RAR;
- System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android);
- 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;
- System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

9. Ochrona przed atakami
   - Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych;
   - System musi 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;
   - Mechanizmy ochrony dla aplikacji internetowych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL injection, trojany, exploity, roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies;
   - Wykrywanie i blokowanie komunikacji C&C do sieci Botnet.
10. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
11. Kontrola aplikacji:
    - Funkcjonalność powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP;
    - Baza kontroli aplikacji powinna zawierać minimum 200 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora;
    - Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików;
    - Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P;
    - Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
12. Kontrola WWW:
    - Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne;
    - W ramach filtra WWW powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: *malware* (lub inne będące źródłem złośliwego oprogramowania), *phishing*, spam, Dynamic DNS, proxy;
    - Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard;
    - Administrator musi mieć 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;
    - Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania;
    - W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
13. Translacja adresów:
    - Translacja adresów NAT: źródłowego i docelowego;

- Translacja PAT;
- Translacja jeden do jeden oraz jeden do wielu;
- Dedykowany ALG (ang. *Application Level Gateway*) dla protokołu SIP.

14. Wirtualizacja i routing dynamiczny:
    - *Policy Routing* realizowany w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego;
    - Protokoły routingu dynamicznego, co najmniej: RIPv2, OSPF, BGP-4 i PIM.
15. Funkcjonalności dla połączeń IPSec VPN:
    - 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;
    - Możliwość wyboru 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.
16. Funkcjonalności dla połączeń SSL VPN:
    - Praca w trybie portalu - 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;
    - Praca w trybie tunelu 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;
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
17. Mechanizmy uwierzytelniania tożsamości użytkowników w ramach sesji:
    - Hasła statyczne i definicje użytkowników przechowywane w lokalnej bazie urządzenia;
    - Hasła statyczne i definicje użytkowników przechowywane w bazach zgodnych z LDAP;
    - Hasła dynamiczne (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych;
    - Mechanizm uwierzytelniania dwuskładnikowego;
    - Mechanizm logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych.
18. Konfiguracja i zarządzanie:
    - Możliwość konfiguracji poprzez terminal i linię komend oraz wbudowaną konsolę graficzną;
    - Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji;
    - Możliwość definiowania wielu administratorów o różnych uprawnieniach;
    - Administratorzy mogą być uwierzytelniani za pomocą:
        - haseł statycznych,
        - haseł dynamicznych (RADIUS, RSA SecureID);
    - System musi umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB.
19. Współpraca z zewnętrznym systemem raportowania i analizy logów umożliwiającym:
    - Zbieranie logów z urządzeń bezpieczeństwa;
    - Generowanie raportów;
    - Skanowanie podatności stacji w sieci;
    - Zdalną kwarantannę dla modułu antywirusowego;
    - Analizę podatności stacji w sieci wraz z możliwością raportowania wykrytych luk.

20. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać certyfikaty ICSA lub równoważne dla funkcji Firewall, IPS, SSL VPN i IPSec VPN.
21. Wykonawca musi dostarczyć bezterminowe licencje aktywacyjne.
22. Wykonawca musi dostarczyć 3-letnie subskrypcje zapewniające automatyczne aktualizacje wszystkich wymienionych funkcjonalności bezpieczeństwa dla oferowanego rozwiązania oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.

Moduł zaawansowanego przetwarzania

1. Architektura modułu:
   - System musi wspierać IPv4 oraz IPv6 w zakresie min. firewall, ochrony w warstwie aplikacji, protokołów routingu dynamicznego;
   - Wymagane jest, by na wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny, Zamawiający uzyskał licencje bez limitu chronionych urządzeń użytkowników (licencje na urządzenie);
   - System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
2. Parametry sprzętowe:
   - Zamawiający nie będzie stosował technologii wirtualizacji domen (ang. *Virtual Domains VDOM*) w rozwiązaniu i nie wymaga dostarczenia tej funkcjonalności;
   - System musi obsługiwać minimum 10 interfejsów sieciowych;
   - System musi wspierać powierzchnię dyskową o pojemności minimum 2 TB;
   - System musi obsługiwać co najmniej 2 rdzenie CPU;
   - System musi obsługiwać co najmniej 4 GB pamięci RAM z możliwością nieograniczonego rozszerzania w górę;
   - W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN-y w oparciu o standard 802.1Q.
3. Wydajność:
   - W zakresie funkcjonalności Firewall obsługa minimum 100 tys. nowych połączeń na sekundę;
   - Przepustowość Firewall: minimum 13 Gbps;
   - Wydajność szyfrowania VPN IPSec (z wykorzystaniem algorytmu AES-256): minimum 1,5 Gbps;
   - Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno po stronie klienta, jak i serwera w ramach modułu IPS) mierzona przy włączonej obsłudze klasy *Stateful Inspection*: minimum 1,5 Gbps;
   - Przepustowość Firewall z włączoną funkcją kontroli aplikacji: minimum 2.6 Gbps;
   - Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus: minimum 1.2 Gbps.
4. Zapewnienie niezawodności:
   - Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych;
   - Monitoring stanu realizowanych połączeń VPN.
5. Dostępne funkcjonalności:
   - Kontrola dostępu - zapora ogniowa klasy *Stateful Inspection*;
   - Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS;
   - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN;
   - Ochrona przed szkodliwym oprogramowaniem *malware* – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS;
   - Ochrona przed atakami (ang. *Intrusion Prevention System*);
   - Kontrola pod kątem rozpoznawania witryn internetowych potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, szpiegujących i generujących spam;
   - Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP;

- Kontrola pasma oraz ruchu (ang. *Quality of Service, Traffic Shaping*) – co najmniej określanie maksymalnej i gwarantowanej ilości pasma;
- Kontrola aplikacji – system musi rozpoznawać aplikacje typu: P2P, Botnet, Proxy Avoidance;
- Możliwość analizy ruchu szyfrowanego protokołem SSL;
- Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

6. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z dwóch trybów: routera z funkcją NAT lub trybie transparentnym (ang. *bridge*).
7. Polityka bezpieczeństwa:
   - Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i zarządzanie pasmem sieci;
   - W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa (np. DMZ, LAN, WAN);
   - Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN (ang. *Software-Defined Networking*): Amazon Web Services (AWS), Microsoft Azure, Cisco ACI, Google Cloud Platform (GCP), OpenStack, VMware vCenter (ESXi); w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
8. Ochrona przed szkodliwym oprogramowaniem *malware*:
   - Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021);
   - System musi umożliwiać skanowanie archiwów, w tym co najmniej ZIP i RAR;
   - System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android);
   - 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;
   - System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Ochrona przed atakami:
   - Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych;
   - System musi 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;
   - Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL injection, trojany, exploity, roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies;
   - Wykrywanie i blokowanie komunikacji C&C do sieci Botnet.
10. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
11. Kontrola aplikacji:
    - Funkcjonalność powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
    - Baza Kontroli Aplikacji powinna zawierać minimum 200 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora;
    - Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików;

- Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P;
- Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

12. Kontrola WWW:
    - Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne;
    - W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: *malware* (lub inne będące źródłem złośliwego oprogramowania), *phishing*, spam, Dynamic DNS, proxy;
    - Filtr WWW musi dostarczać kategorii stron zabronionych prawem, np. hazard.
    - Administrator musi mieć 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;
    - Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania;
    - W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
13. Translacja adresów:
    - Translacja adresów NAT: źródłowego i docelowego;
    - Translacja PAT;
    - Translacja jeden do jeden oraz jeden do wielu;
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
14. Wirtualizacja i routing dynamiczny:
    - *Policy Routing* realizowany w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego;
    - Protokoły routingu dynamicznego, co najmniej: RIPv2, OSPF, BGP-4 i PIM.
15. Funkcjonalności dla połączeń IPSec VPN:
    - 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;
    - Możliwość wyboru 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;
16. Funkcjonalności dla połączeń SSL VPN:
    - Praca w trybie portalu, 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;
    - Praca w trybie tunelu 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;
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
17. Mechanizmy uwierzytelniania tożsamości użytkowników w ramach sesji:
    - Hasła statyczne i definicje użytkowników przechowywane w lokalnej bazie urządzenia;
    - Hasła statyczne i definicje użytkowników przechowywane w bazach zgodnych z LDAP;
    - Hasła dynamiczne (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych;

- Mechanizm uwierzytelniania dwuskładnikowego;
- Mechanizm logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych.

18. Konfiguracja i zarządzanie:
    - Możliwość konfiguracji poprzez terminal i linię komend oraz wbudowaną konsolę graficzną;
    - Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji;
    - Możliwość definiowania wielu administratorów o różnych uprawnieniach;
    - Administratorzy mogą być uwierzytelniani za pomocą:
        - haseł statycznych,
        - haseł dynamicznych (RADIUS, RSA SecureID);
    - System musi umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB.
19. Współpraca z zewnętrznym systemem raportowania i analizy logów umożliwiającym:
    - Zbieranie logów z urządzeń bezpieczeństwa;
    - Generowanie raportów;
    - Skanowanie podatności stacji w sieci;
    - Zdalną kwarantannę dla modułu antywirusowego;
    - Analizę podatności stacji w sieci wraz z możliwością raportowania wykrytych luk.
20. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać certyfikaty ICSA lub równoważne dla funkcji Firewall, IPS, SSL VPN i IPSec VPN.
21. Moduł musi zostać zainstalowany w postaci maszyny wirtualnej w ramach infrastruktury serwerowej Zamawiającego. Zamawiający nie dopuszcza instalacji na serwerach zewnętrznych.
22. Dla zapewnienia pełnej integralności rozwiązania, producentem modułu zaawansowanego przetwarzania powinien być producent oferowanego rozwiązania klastrowego.
23. Wykonawca musi dostarczyć bezterminowe licencje aktywacyjne.
24. Wykonawca musi dostarczyć 3-letnie subskrypcje zapewniające automatyczne aktualizacje wszystkich wymienionych funkcjonalności bezpieczeństwa dla oferowanego rozwiązania oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.

Moduł zbierania i analizy logów

1. Moduł może być dostarczony w postaci dodatkowej funkcjonalności klastra ochrony sieci stanowiąc jego integralny element lub jako odrębne rozwiązanie w postaci sprzętowej lub w postaci maszyny wirtualnej dla środowiska VMware vSphere wraz z odpowiednimi licencjami w postaci elektronicznej.
2. Moduł musi zbierać logi z klastra ochrony sieci i z modułu zaawansowanego przetwarzania.
3. Moduł logowania i raportowania musi stanowić centralne repozytorium danych gromadzonych przez wiele urządzeń oraz aplikacji klienckich z możliwością definiowania własnych raportów na podstawie predefiniowanych wzorców.
4. W przypadku rozwiązania sprzętowego, urządzenie musi zawierać minimum 4 porty GigabitEthernet 10/100/1000.
5. Obsługa powierzchni dyskowej w ramach dostarczonej licencji – minimum 6 TB.
6. Moduł musi obsługiwać (przyjmować logi) dla minimum 9000 urządzeń sieciowych.
7. Rozwiązanie powinno zapewnić przetworzenie minimum 11 GB logów na dzień w ramach dostarczonej licencji.
8. W przypadku rozwiązania w postaci maszyny wirtualnej, rozwiązanie powinno mieć możliwość uruchomienia w środowisku VMware ESX/ESXi 6.5 oraz powinno mieć nielimitowane licencyjnie możliwości zastosowania wirtualnych procesorów oraz wirtualnej pamięci operacyjnej.
9. Moduł zapewnia składowanie oraz archiwizację logów z możliwością ich grupowania według urządzeń i użytkowników.
10. Moduł oferuje możliwość gromadzenia logów w zewnętrznej bazie danych.
11. Moduł musi umożliwiać kwarantannę dla współpracujących z nim urządzeń (kwarantanna obejmuje zainfekowane lub wskazane przez analizę heurystyczną pliki).

12. Moduł zapewnia przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.
13. Moduł zapewnia wyświetlanie nowych logów w czasie rzeczywistym.
14. Moduł musi posiadać funkcjonalność analizowania ruchu w sieci poprzez nasłuch całej komunikacji w segmencie sieci z możliwością jej zapisu i późniejszej analizy.
15. Moduł musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).
16. Moduł musi udostępniać lokalny interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH i konsolę szeregową.
17. Dla zapewnienia pełnej integralności rozwiązania i uproszczenia zarządzania, producentem modułu zbierania i analizy logów powinien być producent oferowanego rozwiązania klastrowego i modułu zaawansowanego przetwarzania.
18. Wykonawca musi dostarczyć bezterminowe licencje aktywacyjne.
19. Wykonawca musi dostarczyć 3-letnie subskrypcje zapewniające automatyczne aktualizacje wszystkich wymienionych funkcjonalności bezpieczeństwa dla oferowanego rozwiązania oraz ciągły dostęp do globalnej bazy.

Wyposażenie dodatkowe

Dla każdego z urządzeń Klastra ochrony sieci Zamawiający wymaga dostarczenia wyposażenia umożliwiającego zestawienie połączeń z istniejącą infrastrukturą sieci Zamawiającego (liczbę sztuk należy pomnożyć przez liczbę urządzeń w klastrze):

- 4 szt. modułów GigabitEthernet ze złączem typu LC, umożliwiających transmisję o prędkości nie mniejszej niż 1 Gbps na dystansie do 300m z wykorzystaniem światłowodu wielodomowego ze złączem typu LC;
- 4 szt. modułów GigabitEthernet ze złączem typu RJ45, umożliwiających transmisję o prędkości nie mniejszej niż 1 Gbps na dystansie do 100m z wykorzystaniem skrętki miedzianej UTP kategorii 5e ze złączem typu RJ45;
- 8 szt. kabli krosowych (ang. *patch cord*) światłowodowych wielomodowych OM3 (MM 50/125) duplex z złączem LC-LC o długości 2m;
- 4 szt. modułów TenGigabitEthernet ze złączem typu LC, umożliwiających transmisję o prędkości nie mniejszej niż 10 Gbps na dystansie do 300m z wykorzystaniem światłowodu wielodomowego ze złączem typu LC.

Dla integracji pojedynczego urządzenia z siecią komputerową Zamawiającego wymagane jest również dostarczenie modułów (liczbę sztuk należy pomnożyć przez liczbę urządzeń w klastrze):

- 8 szt. modułów TenGigabitEthernet ze złączem tylu LC, umożliwiających transmisję o prędkości nie mniejszej niż 10 Gbps na dystansie do 300m z wykorzystaniem światłowodu wielodomowego ze złączem typu LC do posiadanych przez Zamawiającego urządzeń HPE serii 5800 - HP X130 10G SFP+ LC SR Transceiver (JD092B) lub równoważne.

Aktualny system ochrony sieci

Zamawiający użytkuje obecnie centralny system ochrony sieci składający się z:

- 2 urządzeń Fortinet Fortigate 400D pracujących w trybie klastra z aktywnymi usługami i subskrypcjami: Hardware Return To Factory, Firmware & General Updates Web/Online, 24x7 Forticare Contract, AntiVirus Web/Online, NGFW Web/Online, Web Filtering Web/Online i AntiSpam Web/Online.
- 1 instancję Virtual Appliance Fortinet FortiAnalyzer VM64 z licencją na 6 GB logów na dobę oraz 3,5 TB przestrzeni dyskowej z aktywnymi usługami: Firmware & General Updates Web/Online i 24x7 Forticare Contract.

Zamawiający dopuszcza zakup centralnego systemu ochrony sieci w trybie wymiany urządzeń aktualnie użytkowanych przez Zamawiającego.

Gwarancja i usługi serwisowe

1. System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 3 lat, 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.
2. Serwis producenta musi zapewniać możliwość zgłaszania usterek poprzez dedykowany portal lub chat *online* z pracownikiem producenta w trybie 24x7. Dostawca musi zapewnić pierwszą linię wsparcia technicznego telefonicznie w języku polskim w trybie 8 godzin w dni robocze.
3. Producent musi zapewnić w ramach serwisu gwarancyjnego bezpłatny dostęp do najnowszych wydań wewnętrznego oprogramowania urządzeń (ang. *firmware*) przeznaczonych dla oferowanego rozwiązania.
4. Producent musi oferować w ramach serwisu gwarancyjnego bezpłatną wymianę urządzenia w przypadku awarii sprzętowej urządzenia w następnym dniu roboczym w stosunku do dnia zgłoszenia (ang. *Next Business Day*).
5. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać wdrożony system zarządzania jakością w zakresie świadczenia usług serwisowych.

Zakres wymaganych prac

W ramach niniejszego zamówienia wymagana jest realizacja następujących prac w podanej kolejności:

Lp.	Wyszczególnienie	Maksymalny czas realizacji
1.	Projekt wykonawczy	2 tygodnie od podpisania umowy
2.	Dostawa systemu	3 tygodnie od podpisania umowy
3.	Instalacja i konfiguracja systemu	4 tygodnie od podpisania umowy
4.	Optymalizacja systemu	5 tygodni od podpisania umowy
5.	Dokumentacja powdrożeniowa	6 tygodni od podpisania umowy
6.	Instruktaż	7 tygodni od podpisania umowy
7.	Odbiór systemu	8 tygodni od podpisania umowy

Prace wdrożeniowe powinny być przeprowadzone przez uprawnionego inżyniera posiadającego aktualny certyfikat producenta.

Projekt wykonawczy

Przed dostawą Wykonawca przedstawi projekt wykonawczy całej instalacji przygotowany na podstawie wymagań Zamawiającego. Projekt wykonawczy powinien zawierać następujący zakres informacji:

1. Analiza dotychczasowej konfiguracji centralnego systemu ochrony sieci GIG w postaci klastra urządzeń FortiGate 400D ze wskazaniem wymaganych zmian. Należy zweryfikować obiekty w dotychczasowej architekturze i stworzyć obiekty wymagane w nowej architekturze. Projekt powinien zawierać zestawienie dotychczasowych i nowych obiektów.
2. Określenie docelowej konfiguracji interfejsów, VLAN i adresacji IP.
3. Opis integracji nowych urządzeń z siecią LAN GIG. Projekt powinien uwzględniać pracę w układzie klastra niezawodnościowo-wydajnościowego w połączeniu z klastrem HPE IRF.

4. Zasady rozdzielenia ruchu i usług pomiędzy klaster urządzeń i moduł zaawansowanego przetwarzania,.
5. Reguły statycznego i *policy-based* routingu dla nowego systemu.
6. Opracowanie konfiguracji i procedury awaryjnego przejęcia funkcji modułu zaawanasowanego przetwarzania przez klaster urządzeń ochrony sieci.
7. Reguły, obiekty, polityki firewall i profile bezpieczeństwa dla nowego klastra urządzeń ochrony sieci.
8. Opracowanie konfiguracji usług Ipsec VPN i SSL VPN6.
9. Opracowanie reguł zarządzania pasmem.
10. Opis konfiguracji systemu uwierzytelniania użytkowników.
11. Opis konfiguracji integracji klastra urządzeń ochrony sieci i modułu zawansowanego przetwarzania z modułem zbierania i analizy logów.
12. Harmonogram wdrożenia.
13. Opracowanie procedury awaryjnej pozwalającej na bezpieczny powrót do poprzedniej konfiguracji na dotychczasowych urządzeniach Zamawiającego, dla zachowania ciągłości pracy Instytutu w przypadku trudności z przełączeniem na nowe środowisko.

Wszystkie nowe konfiguracje i zmiany w dotychczasowej konfiguracji urządzeń należy przygotować w formie skryptów konfiguracyjnych CLI.

Zamawiający przeanalizuje, oceni jakość i kompletność projektu w terminie do 5 dni roboczych od jego otrzymania. Zaakceptowany przez Zamawiającego projekt będzie podstawą do wdrożenia systemu.

Dostawa systemu

System zostanie dostarczony do Głównego Instytutu Górnictwa w stanie fabrycznie nowym, wolnym od wad technicznych, prawnych i formalnych zwłaszcza w zakresie licencji, uprawnień do aktualizacji oprogramowania *firmware* i zamówionych subskrypcji. Dostawa powinna obejmować wszystkie moduły sprzętowe wraz z dokumentami gwarancyjnymi oraz licencje aktywacyjne oraz subskrypcje zapewniające automatyczne aktualizacje wszystkich wymienionych funkcjonalności bezpieczeństwa dla oferowanego rozwiązania oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.

Instalacja i konfiguracja

Wykonawca przeprowadzi instalację, wstępną konfigurację i włączy system do eksploatacji w GIG. Wstępna konfiguracja obejmować powinna następujące elementy:

- Przygotowanie, na podstawie opisanego przez Zamawiającego rozkładu ruchu w sieci, konfiguracji wykorzystującej w sposób optymalny elementy akceleracji w systemie;
- Przeniesienie danych konfiguracyjnych, wskazanych przez Zamawiającego, do nowego systemu z aktualnego systemu ochrony sieci GIG, w tym między innymi:
    - Konfiguracja interfejsów sieciowych i sieci wirtualnych (VLAN),
    - Konfiguracja ustawień sieciowych i DNS,
    - Polityki firewall wraz z ustawieniami nazw usług, nazw sieciowych i wirtualnych IP,
    - Ustawienia VPN (tunele IPSec oraz portale SSL),
    - Użytkownicy i grupy LDAP oraz lokalni;
- Rozdzielenie funkcji realizowanych obecnie przez klaster urządzeń FortiGate 400D oraz wymaganych nowych funkcjonalności pomiędzy *klaster urządzeń ochrony sieci* oraz *moduł zaawansowanego przetwarzania* według wstępnych założeń:
    - *klaster urządzeń ochrony sieci* realizowałby między innymi funkcje:
        - routingu wewnętrznego pomiędzy sieciami IP GIG,
        - routingu zewnętrznego do Internetu,
        - kontroli ruchu wewnętrznego,
        - kontroli dostępu do wewnętrznych serwerów dla pracowników GIG;

- *moduł zaawansowanego przetwarzania* realizowałby między innymi funkcje:
  - obsługi całego ruchu wychodzącego pracowników do Internetu, w tym filtrowania stron WWW, inspekcji SSL, ochrony antywirusowej, systemu IDS/IPS,
  - serwera proxy dla ruchu wychodzącego pracowników do Internetu,
  - koncentratora SSL VPN,
  - udostępniania usług lokalnych do Internetu z konfiguracją funkcji balansowania;
- Zaprojektowanie i realizacja optymalnego układu połączeń pomiędzy *klastrem urządzeń ochrony sieci, modułem zaawansowanego przetwarzania* oraz rdzeniem sieci na bazie HPE IRF z zapewnieniem wysokiej wydajności, redundancji i odporności na pojedyncze błędy:
  - *klaster urządzeń ochrony sieci* należy połączyć z rdzeniem sieci LAN zbudowanym w oparciu o 4 przełączniki HPE 5820AF 24XG pracujące w połączeniu IRF,
  - połączenia fizyczne należy wykonać przy pomocy światłowodów wielomodowych z dwoma spośród czterech przełączników HPE 5820AF 24XG - na każdym z tych przełączników należy użyć 4 zagregowane (z użyciem protokołu LACP) interfejsy 10 Gbps SFP+,
  - przełączanie ruchu sieciowego podczas awarii powinno przebiegać w możliwie najkrótszym czasie z wykorzystaniem w pełni możliwości, jakie daje HPE IRF oraz *klaster urządzeń ochrony sieci*;
- Przeprowadzenie testów pojedynczych awarii – fizycznego połączenia lub urządzenia dla weryfikacji poprawności konfiguracji;
- Przeprowadzenie w zakresie Firewall procesu optymalizacji reguł przekazanych przez Zamawiającego (polityki, obiekty, zastosowane techniki kontroli w profilach ochronnych);
- Weryfikacja i prezentacja poprawności procesu akceleracji funkcji Firewall oraz IPSec;
- Konfiguracja i optymalizacja systemu zbierania logów z poszczególnych stref bezpieczeństwa oraz zdarzeń zgłaszanych przez *klaster urządzeń ochrony sieci* oraz *moduł zaawansowanego przetwarzania.*

Prace powinny być przeprowadzone w taki sposób, aby zapewnić ciągłość funkcjonowania informatycznych usług w sieci wewnętrznej GIG oraz łączności z Internetem w dni robocze w godzinach pracy (tzn. od 6:00 do 17:00).

Optymalizacja systemu

Na podstawie zebranych statystyk Wykonawca przeprowadzi ostateczną konfigurację i dostrojenie systemu, które obejmować będzie następujące elementy:
- konfiguracja, zgodnie z wymaganiami Zamawiającego, polityki funkcji ochrony zgodnie z dobrymi praktykami producenta dotyczącymi poszczególnych funkcji ochrony;
- przeprowadzenie wszystkich niezbędnych czynności w celu dostosowania pracy systemu do procesu inspekcji ruchu szyfrowanego SSL. System musi poddawać transparentnej inspekcji całą komunikację do sieci Internet z wyjątkiem wskazanych przez Zamawiającego kategorii treści;
- konfiguracja połączenia IPSec z wykorzystaniem elementów akceleracji platformy – tak, aby proces szyfrowania nie wpływał znacząco na obciążenie głównego procesora platformy;
- weryfikacja poprawności pracy urządzenia w konfiguracji odpornej na awarie (HA) – w szczególności podtrzymanie aktywnych sesji w momencie przełączenia węzłów klastra.

Dokumentacja powdrożeniowa

Wykonawca przygotuje dokumentację powdrożeniową, która powinna obejmować:
1. Opis konfiguracji sprzętowej klastra HA wraz z konfiguracją sprzętową urządzeń zależnych;
2. Opis konfiguracji sieciowej (konfiguracja portów, akceleracja portów, adresy IP, VLAN, itd.) klastra HA oraz urządzeń zależnych;
3. Opis sposobu integracji wdrożonego systemu z istniejącymi u Zamawiającego systemami (usługi katalogowe, systemy autentykacji, itd.);
4. Opis zakresu poszczególnych stref bezpieczeństwa oraz sposobu przydzielania dostępu do określonych stref;
5. Opis polityk bezpieczeństwa w poszczególnych strefach bezpieczeństwa;
6. Opis zastosowanego sposobu zarządzania pasmem w poszczególnych politykach bezpieczeństwa;

7. Opis funkcji ochronnych i ich konfiguracji zastosowanych w poszczególnych politykach bezpieczeństwa;
8. Opis konfiguracji zapisywania logów, raportowania zdarzeń i współpracy z programem zarządzającym siecią;
9. Opis konfiguracji dostępu szyfrowanego VPN w trybach Site-to-Site oraz Client-to-Site;
10. Opis konfiguracji modułu zaawansowanego przetwarzania;
11. Opis konfiguracji modułu zbierania i analizy logów;
12. Źródła pomocy technicznej: adresy internetowe wsparcia technicznego, adresy i telefony serwisu gwarancyjnego i pogwarancyjnego.

Instruktaż

Instruktaż powinien zostać przeprowadzony w siedzibie Zamawiającego dla max. 6 pracowników Zamawiającego w terminach uzgodnionych z Zamawiającym.

Zakres instruktażu:

- Ogólny opis systemu, interfejs graficzny i polecenia CLI;
- Podstawowe działania konfiguracyjne (konfiguracja portów, VLAN, routingu, itp.);
- Konfiguracja stref bezpieczeństwa oraz skorelowanych z nimi polityk bezpieczeństwa;
- Konfiguracja zarządzania pasmem;
- Integracja systemu z systemem katalogowym oraz systemami autentykacyjnymi;
- konfiguracja funkcji bezpieczeństwa (Antivirus, IPS, Application Control, Web Filtering, Antispam, DLP, itp.);
- Konfiguracja dostępu VPN w trybach Site-to-Site oraz Client-to-Site;
- Konfiguracja modułu zaawansowanego przetwarzania;
- Konfiguracja modułu zbierania i analizy logów oraz zdarzeń zbieranych z urządzenia;
- Symulacja co najmniej 2 ataków sieciowych i analiza reakcji systemu IPS;
- Zaawansowane metody diagnostyczne (*debugging*, *sniffing*, itp.).

Czas trwania instruktażu: minimum 8h (2 dni x 4 h).

Odbiór systemu

Odbiór systemu może zostać przeprowadzony po realizacji pełnego zakresu wymaganych prac. Przy odbiorze Wykonawca przekazuje Zamawiającemu aktualną dokumentację powdrożeniową w wersji papierowej i elektronicznej.

Należy podać:

- **Cenę netto w PLN / brutto w PLN (cena winna obejmować koszty opakowania, transportu i ubezpieczenia od Wykonawcy do Zamawiającego) oraz stawkę i wartość podatku VAT,**
- **Wykonawca zobowiązany jest do wypełnienia wszystkich pustych pól formularza ofertowego. Wykonawca zobowiązany jest do podania wszystkich komponentów oferowanego rozwiązania (sprzęt, oprogramowanie, wyposażenie, usługi) w sposób umożliwiający ich jednoznaczną identyfikację.**

Wstępną ofertę należy złożyć na załączniku nr 1

Miejsce i termin składania ofert wstępnych:

Wstępną ofertę należy złożyć do dnia **23.11.2021. do godziny 12:00** drogą elektroniczną lub w siedzibie Zamawiającego:

Główny Instytut Górnictwa
Dział Handlowy (FZ-1)
Plac Gwarków 1
40-166 Katowice

adres e-mail: makolczyk@gig.eu

Kontakt handlowy:

mgr inż. Marzena Kolczyk - tel. (32) 259 23 42, e-mail: **makolczyk@gig.eu**

ZAPRASZAMY DO SKŁADANIA OFERT

Z poważaniem,

Zastępca Kierownika Działu Handlowego

mgr Monika Wallenburg

GŁÓWNY INSTYTUT GÓRNICTWA Jednostka Notyfikowana nr 1453

Plac Gwarków 1
40-166 Katowice
gig.eu

T: 32 259 20 00
F: 32 259 65 33
E: gig@gig.eu

Konto: 05 1140 1078 0000 3018 1200 1001
Regon: 000023461, NIP: 6340126016
KRS: 0000090660

Certyfikowany Zintegrowany System Zarządzania
spełnia wymagania norm: PN-EN ISO 9001:2015-10
PN-ISO 45001:2018-06, PN-EN ISO 14001:2015-09

Załącznik nr 1

Wstępna oferta na dostawę wdrożenie oraz serwis Centralnego Systemu Ochrony Sieci.

Nazwa/Imię i Nazwisko Wykonawcy:
.....
Adres: .....
Nr tel.: .....
Adres e-mail: .....
Osoba do kontaktu: .....
Oferujemy wykonanie przedmiotu zamówienia zgodnie z warunkami zawartymi we wstępnym zapytaniu ofertowym za cenę:

Lp.	Przedmiot zamówienia wskazany we wstępnym zapytaniu	Nazwa producenta	Opis produktu/usługi	Identyfikatory P/N	Jedn. miary	Ilość	Cena jedn. (netto) w PLN	Wartość ogółem (netto) w PLN	Stawka (%) podatku VAT	Kwota podatku VAT w PLN	Wartość ogółem (brutto) w PLN
1	2	3	4	5	6	7	8	9	10	11	12
1.	Urządzenie ochrony sieci (sprzęt + 36 mies. kontrakt serwisowy)				szt.						
2.	Moduł zaawansowanego przetwarzania (oprogramowanie + 36 mies. maintenance)				szt.						
3.	Moduł zbierania i analizy logów – (oprogramowanie + 36 mies. maintenance)				szt.						
4.	Moduł GigabitEthernet for UTM LC MM 300m				szt.						
5.	Moduł GigabitEthernet for UTM RJ45 UTP 5e 100m				szt.						
6.	Kabel krosowy światłowodowy OM3 (MM 50/125) duplex LC-LC 2m				szt.						
7.	Moduł TenGigabitEthernet for UTM SFP+ LC 300m				szt.						
8.	Moduł TenGigabitEthernet for HPE SFP+ LC-SR Transceiver 300m				szt.						
9.	Projekt wykonawczy	X		X	szt.						
10.	Dostawa systemu	X		X	szt.						
11.	Instalacja i konfiguracja	X		X	szt.						

12.	Optymalizacja systemu	X		X	szt.						
13.	Instruktaż	X		X	szt.						
14.	Dokumentacja powdrożeniowa	X		X	szt.						
RAZEM:									X		

Wykonawca zobowiązany jest do wypełnienia wszystkich pustych pól powyższego formularza. Wykonawca zobowiązany jest do podania wszystkich komponentów oferowanego rozwiązania (sprzęt, oprogramowanie, wyposażenie, usługi) w sposób umożliwiający ich jednoznaczną identyfikację.

OŚWIADCZENIE RODO DLA WYKONAWCY

1. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

- administratorem danych osobowych **WYKONAWCY** jest: *Główny Instytut Górnictwa, Plac Gwarków 1,40 - 166 Katowice,*
- inspektorem ochrony danych osobowych w *Głównym Instytucie Górnictwa* jest Pani: *mgr Katarzyna Kareł, e-mail:* gdpr@gig.eu.
- dane osobowe **WYKONAWCY** przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym wstępnym zapytaniem ofertowym,
- odbiorcami danych osobowych **WYKONAWCY** będą osoby lub podmioty, którym udostępniona zostanie dokumentacja dotycząca niniejszego wstępnego zapytania ofertowego,
- dane osobowe **WYKONAWCY** będą przechowywane przez okres 4 lat,
- w odniesieniu do danych osobowych **WYKONAWCY** decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- **WYKONAWCA** posiada :
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych dotyczących **WYKONAWCY** ;
  - na podstawie art. 16 RODO prawo do sprostowania danych osobowych **WYKONAWCY** ;
  - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO ;
  - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy **WYKONAWCA** uzna, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- **WYKONAWCY** nie przysługuje:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
  - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
  - **na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania danych osobowych WYKONAWCY jest art. 6 ust. 1 lit. c RODO**.

.....
Miejscowość, data

.....
Podpis