Instytut Badawczy

Nr sprawy: **FZ-1/5510/MKO/21** **Katowice, 04.03.2021 r.**

Dotyczy : Wstępnego zapytania ofertowego w celu ustalenia wartości zamówienia dla planowanego postępowania przetargowego

Szanowni Państwo,

Zwracamy się z prośbą o wstępną ofertę na dostawę, instalację oraz instruktaż dla Centralnego Systemu Ochrony Sieci.

Centralny System Ochrony Sieci musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa, niezależnie od dostawcy łącza sieciowego. System ten powinien 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. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Platformy wirtualne muszą wspierać następujące rodzaje hypervisorów: ESXi v5.5 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.

Klaster urządzeń ochrony sieci

1. Architektura systemu ochrony:
   - 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 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 powinien zostać dostarczony w postaci klastra HA (ang. *High Availability*).
2. Ilość/rodzaj portów dla pojedynczego urządzenia:
   - 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, powinien być wyposażony w odpowiedni moduł połączeniowy, w pełni kompatybilny z urządzeniem:

- 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;
- 2 szt. kabli krosowych (ang. *patch cord*) światłowodowych wielomodowych OM3 (MM 50/125) duplex z złączem LC-LC o długości 2m;

- Każdy z portów typu SFP+, powinien być wyposażony w odpowiedni moduł połączeniowy, w pełni kompatybilny z urządzeniem:
  - 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;
- 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 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 powinien 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 powinien dawać możliwość pracy w jednym z dwóch trybów: rutera 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 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 powinien 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 Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
   - Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
10. Silnik antywirusowy powinien 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:

- Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 2 wirtualnych zapór, gdzie każda z nich posiada indywidualne ustawienia wszystkich funkcji bezpieczeństwa i dostęp administracyjny;
- *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 *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;
    - Praca 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;
    - 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 powinien 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 powinien dostarczyć licencje aktywacyjne oraz subskrypcje zapewniające automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL, przez okres 3 lat.

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:
   - 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 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 powinien 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 powinien dawać możliwość pracy w jednym z dwóch trybów: rutera 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 *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 powinien 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 Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies;
   - Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
10. Silnik antywirusowy powinien 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:
    - Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 2 wirtualnych zapór, gdzie każda z nich posiada indywidualne ustawienia wszystkich funkcji bezpieczeństwa i dostęp administracyjny;
    - *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 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;
    - Praca 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;
    - 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 powinien 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 powinien dostarczyć licencje aktywacyjne oraz subskrypcje zapewniające automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL, przez okres 3 lat.

Moduł zbierania i analizy logów

1. Architektura modułu:
   - 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;
   - Moduł powinien zbierać logi z klastra ochrony sieci;

- Moduł logowania i raportowania powinien stanowić centralne repozytorium danych gromadzonych przez wiele urządzeń oraz aplikacji klienckich z możliwością definiowania własnych raportów na podstawie predefiniowanych wzorców.

2. Parametry fizyczne modułu:
   - W przypadku rozwiązania sprzętowego, urządzenie musi zawierać minimum 4 porty GigabitEthernet 10/100/1000;
   - Obsługa powierzchni dyskowej w ramach dostarczonej licencji – minimum 6 TB;
   - Moduł musi obsługiwać (przyjmować logi) dla minimum 9000 urządzeń sieciowych;
   - Rozwiązanie powinno zapewnić przetworzenie minimum 6 GB logów na dzień w ramach dostarczonej licencji;
   - W przypadku rozwiązania w postaci maszyny wirtualnej, rozwiązanie powinno mieć możliwość uruchomienia w środowisku VMware ESX/ESXi 6.5 oraz powinna mieć nielimitowane licencyjnie możliwości zastosowania wirtualnych procesorów oraz wirtualnej pamięci operacyjnej.
3. Funkcjonalności modułu:
   - Składowanie oraz archiwizacja logów z możliwością ich grupowania według o urządzeń i użytkowników;
   - Możliwość gromadzenia logów w zewnętrznej bazie danych;
   - Kwarantanna dla współpracujących z nim urządzeń (kwarantanna obejmuje zainfekowane lub wskazane przez analizę heurystyczną pliki);
   - Przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących;
   - Wyświetlanie nowych logów w czasie rzeczywistym;
   - Analizowanie ruchu w sieci poprzez nasłuch całej komunikacji w segmencie sieci z możliwością jej zapisu i późniejszej analizy;
   - Export zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych);
   - Moduł musi udostępniać lokalny interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH i konsolę szeregową.

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, Enhanced Support 8x5, AntiVirus Web/Online, NGFW Web/Online, Web Filtering Web/Online i AntiSpam Web/Online. Usługi i subskrypcje są dostępne do 30 kwietnia 2021 r.
- 1 instancję Virtual Appliance Fortinet FortiAnalyzer VM64 z licencją na 6GB logów na dobę oraz 3,5 TB przestrzeni dyskowej z aktywnymi usługami: Firmware & General Updates Web/Online i Enhanced Support oraz Telephone Support 24x7. Usługi są dostępne do 30 kwietnia 2021 r.

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

Gwarancja i usługi serwisowe

1. System powinien 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 powinien zapewniać możliwość zgłaszania usterek poprzez dedykowany portal lub chat *online* z pracownikiem producenta w trybie 24x7. Dostawca powinien zapewnić pierwszą linię wsparcia technicznego telefonicznie w języku polskim w trybie 8 godzin w dni robocze.
3. Producent powinien zapewnić w ramach serwisu gwarancyjnego bezpłatny dostęp do najnowszych wydań wewnętrznego oprogramowania urządzeń (ang. *firmware*) przeznaczonych dla oferowanego rozwiązania.
4. Producent powinien oferować w ramach serwisu gwarancyjnego bezpłatną wymianę urządzenia w przypadku poważniejszej usterki sprzętowej.
5. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący powinien 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.	**Dostawa systemu**	**3 tygodnie od podpisania umowy**
2.	**Instalacja i konfiguracja systemu**	**4 tygodnie od podpisania umowy**
3.	**Optymalizacja systemu**	**5 tygodni od podpisania umowy**
4.	**Dokumentacja powdrożeniowa**	**6 tygodni od podpisania umowy**
5.	**Instruktaż**	**7 tygodni od podpisania umowy**
6.	**Odbiór systemu**	**8 tygodni od podpisania umowy**

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

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 sygnatur ataków, aplikacji, szczepionek antywirusowych 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;
- 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 urządzenie.

Przed instalacją Wykonawca przedstawi projekt wykonawczy całej instalacji przygotowany na podstawie wymagań Zamawiającego. Projekt po akceptacji przez Zamawiającego będzie podstawą do wdrożenia.

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 powinien 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. 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 zbierania i analizy logów oraz zdarzeń zbieranych z urządzenia;
- symulacja co najmniej 2 ataków sieciowych i analiza reakcji systemu IPS;
- zaawansowane metody diagnostyczne (debuging, 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,**
- **Warunki płatności.**

Wstępną ofertę należy złożyć na załączniku nr 1

Miejsce i termin składania ofert

Wstępną ofertę należy złożyć do dnia **10.03.2021. 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 Monika Wallenburg - tel. (32) 259 25 47, e-mail: **mwallenburg@gig.eu**
mgr inż. Marzena Kolczyk - tel. (32) 259 23 42, e-mail: **makolczyk@gig.eu**

ZAPRASZAMY DO SKŁADANIA OFERT

Z poważaniem,

Kierownik Działu Handlowego

mgr Monika Wallenburg

Nr sprawy: Nr sprawy: **FZ-1/5510/MKO/21**

Załącznik nr 1

Wstępna oferta na dostawę, instalację oraz instruktaż dla 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.	Nazwa zaoferowanego systemu*	Jednostka 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
1								
RAZEM :								

- Warunki płatności: .....

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