**ZP/92/2023**

**AKTUALIZACJA**

|  |
| --- |
| **Szczegółowy opis przedmiotu zamówienia** |

Do obowiązków wykonawcy w ramach realizacji Pakietu należeć będzie: dostawa, instalacja i konfiguracja Hardware oraz Software w zakresie:

1. Dostawa, instalacja oraz konfiguracja Systemu Bezpieczeństwa (UTM – Unified Threat Menegement) wraz z usługą instalacji oraz konfiguracji
2. ~~Usługa testowego odtwarzania kopii bezpieczeństwa~~
3. ~~Audyt bezpieczeństwa – w ramach finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców~~
4. **Wymagania na dostawę i instalację oraz konfigurację Systemu Bezpieczeństwa (UTM)** **Unified Threat Menegement) wraz z usługą instalacji oraz konfiguracji:**

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa, instalacja i konfiguracja systemu bezpieczeństwa. Wymagania dotyczące Systemu Bezpieczeństwa:

## **Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od łącza dostawcy. Dopuszcza się 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.

Wykonawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych fizycznych instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu.

**System musi wspierać IPv4 oraz IPv6 w zakresie:**

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

## **Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

## **Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:
* 1 port Gigabit Ethernet RJ-45
* 1 port 2.5 Gigabit Ethernet RJ-45
* 8 portów 10 GE RJ45
* 16 gniazd 10 GE SFP+
* 8 gniazd 25 GE SFP28
* 2 gniazda 100GE QSFP28
1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz dwa gniazda USB oraz możliwość instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w redundantne zasilanie AC.

## **Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 7,5 mln jednoczesnych połączeń oraz 650.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 196 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 134 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 44 Gbps.
5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 55 Gbps.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 19 Gbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 13 Gbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 10 Gbps.

## **Funkcje Systemu Bezpieczeństwa:**

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.
13. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

## **Polityki, Firewall**

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

## **Połączenia VPN**

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
* 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.
1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

## **Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
* Routingu statycznego.
* Policy Based Routingu.

·  Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

1. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

## **Zarządzanie pasmem**

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

## **Kontrola Antywirusowa**

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

## **Ochrona przed atakami**

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Ochrana przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. 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.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

## **Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

## **Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. 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 avoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

## **Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
* 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.
1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

## **Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

## **Logowanie**

1. System musi 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, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

## **Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

* ICSA lub EAL4 dla Firewall.
* ICSA lub NSS Labs dla funkcji IPS.
* ICSA dla funkcji IPSec VPN.
* ICSA dla funkcji SSL VPN.

## **Serwisy i licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

* Kontrola Aplikacji,
* IPS,
* Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android),
* Analiza typu Sandbox,
* Antyspam,
* Web Filtering,
* bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

## **Gwarancja oraz wsparcie**

**System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.**

## **Zakres usług dodatkowych do jakich jest zobowiązany Wykonawca:**

1. Podłączenie i uruchomienie:
* aktualizacja firmware
* konfiguracja klastra HA
1. Konfiguracja sieciowa:
* konfiguracja interfejsów
* konfiguracja routingu
1. Konfiguracja obiektów i modułów bezpieczeństwa:
* konfiguracja obiektów wykorzystywanych w regułach firewall'a na podstawie listy dostarczonej przez Zamawiającego
* konfiguracja modułów bezpieczeństwa (Antivirus, WebFiltering, DNS Filtering, IPS, Antispam)
* konfiguracja reguł zapory sieciowej (w tym firewall + DoS policy)
1. Konfiguracja VPN:
* konfiguracja tuneli VPN IPSec stite-to-site
* konfiguracja tuneli dialup (SSL VPN, VPN IPSec)
1. Konfiguracja logowania
2. Weryfikacja poprawnej pracy systemu

Wykonawca, zobowiązany jest załączyć do **OFERTY** – **Przedmiotowe środki dowodowe.**

Szczegółowe wytyczne w zakresie przedmiotowych środków dowodowych zawarte są w pkt. VI SWZ.

*UWAGA: Ilekroć w dokumentacji, wskazano markę lub pochodzenie produktu lub urządzenia, należy przyjąć, że za każdą nazwą jest umieszczone słowo „lub równoważne”, tzn. że wbudowane materiały, urządzenia itp. będą posiadały (charakteryzowały się) wszystkimi parametrami nie gorszymi niż opisane w niniejszej dokumentacji.*

***Jeżeli w opisie przedmiotu zamówienia wskazane są konkretne rozwiązania techniczne, dopuszcza się stosowanie rozwiązań równoważnych, co do ich cech i parametrów – określonych dla pozycji przedmiotu zamówienia, a wszystkie ewentualne nazwy firmowe urządzeń i wyrobów użyte w opisie przedmiotu zamówienia powinny być traktowane jako definicje standardowe, a nie konkretne nazwy firmowe urządzeń, wyrobów zastosowanych w niniejszej dokumentacji. Obowiązek udowodnienia równoważności leży po stronie Wykonawcy****.*

**Aktualizacja z dnia 18.09.2023 r. – dotyczy specyfikacji w zakresie przedmiotu zamówienia do realizacji.**

Przedmiotem zamówienia jest **dostawa**, instalacja oraz konfiguracja Systemu Bezpieczeństwa (UTM – Unified Threat Menegement) wraz z usługą instalacji oraz konfiguracji.

**W zakres przedmiotowej dostawy nie wchodzą usługi:**

* Usługa testowego odtwarzania kopii bezpieczeństwa
* Audyt bezpieczeństwa – w ramach finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców