Załącznik nr 1 do Zapytania

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa dwóch zapór sieciowych dla MZ.

Termin realizacji zamówienia:

do 50 dni roboczych od dnia zawarcia Umowy

Przedmiot zamówienia:

Zamówienie obejmuje:

a. Dostawę Urządzeń i oprogramowania opisanych szczegółowo w pkt. 1.
b. Dostawa zostanie zrealizowana do ośrodków przetwarzania danych Zamawiającego zlokalizowanych na terenie Warszawy.
c. Gwarancję na warunkach opisanych w pkt.2 .

Wymagania ogólne:

a. Wszystkie dostarczone Urządzenia zasilane prądem przemiennym muszą być zasilane napięciem 230 V/50 Hz.
b. Zamawiający wymaga, aby dostarczone Urządzenia były fabrycznie nowe (tzn. bez śladów używania i uszkodzenia, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Rzeczpospolitej Polskiej.
c. Oferowane Urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
d. Wszystkie wymagane moduły SFP, SFP+, SFP28, QSFP muszą być producentów urządzeń.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

1. Zapora ogniowa typ 1

Dostawa 2 urządzeń, każde o wymaganiach opisanych poniżej.

1.1. 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.
1.2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
1.3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
1.4. Monitoring stanu realizowanych połączeń VPN.
1.5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
1.6. System realizujący funkcję Firewall musi dysponować minimum:
1.7. 10 portami Gigabit Ethernet RJ-45.
1.8. 8 gniazdami SFP 1 Gbps.
1.9. 2 gniazdami SFP+ 10 Gbps.
1.10. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
1.11. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
1.12. System realizujący funkcję Firewall musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 480 GB.
1.13. System musi być wyposażony w zasilanie AC.
1.14. W zakresie Firewall'a obsługa nie mniej niż 8 mln. jednoczesnych połączeń oraz 450 tys. nowych połączeń na sekundę.
1.15. Przepustowość Stateful Firewall: nie mniej niż 36 Gbps dla pakietów 512 B.
1.16. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 15 Gbps.
1.17. Wydajność szyfrowania IPSec VPN nie mniej niż 20 Gbps.
1.18. 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 10 Gbps.
1.19. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 7 Gbps.
1.20. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 8 Gbps.
1.21. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
   a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
   b) Kontrola Aplikacji.
   c) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
   d) Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
   e) Ochrona przed atakami - Intrusion Prevention System.
   f) Kontrola stron WWW.
   g) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
   h) Zarządzanie pasmem (QoS, Traffic shaping).
1.22. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

1.23. 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 dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
1.24. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
1.25. Analiza ruchu szyfrowanego protokołem SSH.
1.26. 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
1.27. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
1.28. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   a) Translację jeden do jeden oraz jeden do wielu.
   b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
1.29. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
1.30. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
1.31. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   a) Amazon Web Services (AWS).
   b) Microsoft Azure
   c) Google Cloud Platform (GCP).
   d) OpenStack.
   e) VMware NSX.
1.32. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   a) Wsparcie dla IKE v1 oraz v2.
   b) Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   c) Obsługa protokołu Diffie-Hellman grup 19 i 20.
   d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   h) Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   i) Mechanizm „Split tunneling” dla połączeń Client-to-Site.
1.33. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   a) 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.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
c) Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

1.34. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
a) Routingu statycznego.
b) Policy Based Routingu.
c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

1.35. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

1.36. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

1.37. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

1.38. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

1.39. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

1.40. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

1.41. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

1.42. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

1.43. 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.

1.44. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

1.45. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

1.46. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

1.47. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

1.48. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

1.49. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

1.50. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

1.51. 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.

1.52. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

1.53. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

1.54. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

1.55. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

1.56. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
1.57. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
1.58. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
1.59. 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.
1.60. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
1.61. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
1.62. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
1.63. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
1.64. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
1.65. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
1.66. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
1.67. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
1.68. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
1.69. 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.
1.70. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
1.71. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
1.72. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
1.73. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
1.74. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
1.75. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
1.76. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

1.77. 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.

1.78. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

1.79. Musi istnieć możliwość logowania do serwera SYSLOG.

1.80. Wyposażenie dodatkowe na urządzenie:

a) 2 wkładki 10G SFP+ SR
b) 8 wkładek 1G SFP SR

1.81. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

a) ICSA lub EAL4 dla funkcji Firewall.

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

a) 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 36 miesięcy.

2. Gwarancja

2.1 Dostawca gwarantuje, że każdy produkt, który zostanie dostarczony jest fabrycznie nowy i pochodzi bezpośrednio od producenta lub autoryzowanego sprzedawcy.

2.2 Urządzenia muszą być objęte przynajmniej 36 miesięczną gwarancją od dnia podpisania Protokołu Odbioru wnioskującego o rozliczenie finansowe. Zamawiający dopuszcza świadczenie gwarancji bezpośrednio przez producenta lub partnera producenta przy wsparciu producenta w reżimie 8x5xNBD (tj. 8 godzin w dni robocze) uprawniającym do wsparcia telefonicznego i mailowego w zakresie konfiguracji Urządzenia oraz dającym prawo do aktualizacji oprogramowania, a w przypadku ujawnienia wad w okresie gwarancji Wykonawca w ramach gwarancji zobowiązuje się w terminie nie dłuższym niż 5 dni roboczych od dnia zgłoszenia tego faktu przez Zamawiającego (reklamacja) do:

a) usunięcia wad Urządzenia w siedzibie Zamawiającego lub, jeżeli usunięcie wady w siedzibie nie jest możliwe, usunięcia wady poza siedzibą Zamawiającego. W przypadku, gdy Wykonawca wykonuje naprawę poza siedzibą Zamawiającego, jest on zobowiązany na czas naprawy udostępnić Zamawiającemu i dostarczyć na własny koszt sprzęt zastępczy o parametrach nie gorszych od Urządzenia naprawianego. Koszty związane z dostarczeniem urządzenia zastępczego ponosi Wykonawca;
b) wymiany Urządzenia na nowe, wolne od wad.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706