Znak sprawy: BA.WZP.26.40.2024

Załącznik nr 1 do SWZ

Opis przedmiotu zamówienia (OPZ)

System bezpieczeństwa

Czas trwania umowy

12 miesięcy.

Urządzenia systemu bezpieczeństwa

Wymagania ogólne

System składa się z trzech elementów: urządzeń Firewall zgodnych ze specyfikacją zawartą poniżej, zintegrowanego z Firewallami systemu centralnego zarządzania oraz zintegrowanego z Firewallami systemu centralnego uwierzytelniania. Całość musi współpracować z posiadanym i wdrożonym przez Zamawiającego systemem Firewall Fortigate 601E.

Urządzenia bezpieczeństwa realizują wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

1. Dostawa sprzętu

Wymagania dla elementów pełniących funkcję firewall

1. Każde urządzenie musi obsługiwać funkcjonalność automatycznej konfiguracji we współpracy z centralnym zarządzaniem będącym elementem oferty.
2. Oferowane firewall'e muszą mieć opcję automatycznej aktualizacji swojego oprogramowania z możliwą konfiguracją czasu wykonania oraz ilości dni zwłoki po udostępnieniu nowej wersji przez producenta.
3. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów:
   3.1. Routera z funkcją NAT,
   3.2. transparentnym
   3.3. monitorowania kopii ruchu dostarczonej do interfejsu urządzenia.
4. Urządzenie umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.
   4.1. Musi istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji urządzenia.
5. Urządzenie wspiera protokoły IPv4 oraz Ipv6 w zakresie:
   5.1. Firewall
   5.2. Ochrony w warstwie aplikacji
   5.3. Protokołów routingu dynamicznego.
6. Redundancja, monitoring i wykrywanie awarii:
   6.1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji
   6.2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych

6.3. Monitoring stanu realizowanych połączeń VPN
6.4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

7. W zakresie routingu rozwiązanie zapewnia obsługę:
   7.1. Routingu statycznego.
   7.2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
   7.3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
   7.4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
   7.5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
   7.6. BFD (Bidirectional Forwarding Detection).
   7.7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
8. Funkcje SD-WAN
   8.1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
   8.2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
9. Zarządzanie pasmem
   9.1. Urządzenie Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
   9.2. Urządzenie daje możliwość określania pasma dla poszczególnych aplikacji.
   9.3. Urządzenie pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
10. Urządzenie zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
11. Podstawowe funkcje zabezpieczeń:
   11.1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
   11.2. Kontrola Aplikacji.
   11.3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN
   11.4. Ochrona przed atakami - Intrusion Prevention System
   11.5. Zarządzanie pasmem (QoS, Traffic shaping).
   11.6. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
   11.7. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
   11.8. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
   11.9. Polityka Firewall musi uwzględniać co najmniej parametry: strefy bezpieczeństwa, adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń na początku nawiązywania połączenia i na końcu.
   11.10. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
      11.10.1. Translację jeden do jeden oraz jeden do wielu.
      11.10.2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
   11.11. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
   11.12. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.

11.13. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

11.14. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

11.15. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

11.15.1. Amazon Web Services (AWS).

11.15.2. Microsoft Azure.

11.15.3. Cisco ACI.

11.15.4. Google Cloud Platform (GCP).

11.15.5. OpenStack.

11.15.6. VMware NSX.

11.15.7. Kubernetes.

11.16. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

11.16.1. Wsparcie dla IKE v1 oraz v2.

11.16.2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).

11.16.3. Obsługa protokołu Diffie-Hellman grup 19, 20.

11.16.4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.

11.16.5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

11.16.6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

11.16.7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

11.16.8. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.

11.16.9. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.

11.16.10. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.

11.16.11. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.

11.16.12. Mechanizm „Split tunneling” dla połączeń Client-to-Site.

11.17. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

11.17.1. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.

11.17.2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

11.18. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

11.19. Ochrona przed atakami sieciowymi musi spełniać szczegółowe wymagania:

11.19.1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

11.19.2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.

11.19.3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

11.19.4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.

11.19.5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
11.19.6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
11.19.7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
11.19.8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
11.19.9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

11.20. Kontrola aplikacji musi umożliwiać co najmniej:
11.20.1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
11.20.2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
11.20.3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
11.20.4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
11.20.5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
11.20.6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
11.20.7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

11.21. Uwierzytelnianie użytkowników w ramach sesji firewall musi spełniać minimalne wymagania:
11.21.1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
11.21.2. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
11.21.3. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
11.21.4. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
11.21.5. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
11.21.6. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
11.21.7. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

12. Funkcje zabezpieczeń, które urządzenie ma realizować – jeśli jest wymagana licencja należy ja dostarczyć na okres tożsamy z wymaganym wsparciem serwisowym:
12.1. Ochrona przed malware
12.2. Kontrola kategorii odwiedzanych stron WWW
12.3. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
12.4. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Ochrona przed malware musi spełniać następujące wymagania szczegółowe:
13.1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

13.2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
13.3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
13.4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
13.5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
13.6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
13.7. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
13.8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
13.9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

14. Kontrola ruchu WWW musi spełniać wymagania:
14.1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
14.2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
14.3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
14.4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
14.5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
14.6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
14.7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
14.8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
14.9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

15. Zarządzanie
15.1. Wszystkie elementy firewall systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i muszą współpracować z dedykowanymi platformami centralnego zarządzania, monitorowania i zarządzania logami, które to muszą być zawarte w ofercie w części podstawowej.
15.2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
15.3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
15.4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
15.5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

15.6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

15.7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

15.8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).

15.9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

16. Logowanie

16.1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

16.2. Musi istnieć opcja logowanie do aplikacji udostępnianej w chmurze tego samego producenta.

16.3. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

16.4. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.

16.5. Musi istnieć możliwość włączenia logowania per reguła w polityce firewall w zakresie: rozpoczęcie połączenia, zakończenie połączenia, wszystkie logi lub tylko zdarzenia profili bezpieczeństwa.

16.6. System zapewnia możliwość logowania do serwera SYSLOG.

16.7. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołów: UDP, TCP oraz szyfrowania SSL/TLS.

17. Gwarancja oraz wsparcie dla sprzętowych firewalli:

17.1. System jest objęty serwisem gwarancyjnym producenta, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.

17.2. W ramach serwisu gwarancyjnego producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Urządzenia firewall

Ilość wymaganych sztuk w ofercie: 16

1. Właściwości fizyczne urządzenia:

1.1. 6 portów GigabitEthernet RJ45

1.2. 2 gniazda SFP 1Gbps.

1.3. Wbudowany modem 3G/4G LTE z 2 slotami SIM działającymi w trybie Active-Passive. Modem musi posiadać złącza do podłączenia anten zewnętrznych. Anteny są elementem podstawowym zestawu.

1.4. Port USB do ewentualnego podłączenia dodatkowego modemu oraz instalacji oprogramowania

1.5. Port szeregowy ze złączem RJ45

1.6. Port konsolowy RJ45

1.7. Moduł I/O do komunikacji fizycznej alarmów

1.8. Wbudowany moduł szyfrowania TPM (*Trusted Platform Module*)

1.9. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q

1.10. Temperatura dopuszczanego środowiska pracy systemu mieści się w zakresie: -40°C - 75°C.

1.11. System ma zostać dostarczony wraz z zasilaczem 230V.

1.12. Zamawiający wymaga dostarczenia do każdego oferowanego urządzenia zasilacza kompatybilnego z oferowanym urządzeniem.
   a. Zasilacz musi mieć minimum 50% zapasu mocy względem mocy maksymalnej oferowanego urządzenia, zapewniającego jego stabilną pracę.
   b. Zasilacz musi pracować w zakresie temperatur minimum -20 +60 st.C
   c. Zasilacz musi mieć możliwość bezpośredniej instalacji na szynie DIN.
   d. Zasilacz nie może posiadać aktywnego chłodzenia
   e. Zabezpieczenie przeciwzwarciowe, przeciążeniowe, nadnapięciowe
   f. Zgodność z normami i certyfikatami obowiązującymi na terenie Polski

1.13. Wraz z kompatybilnym względem oferowanego urządzenia zasilaczem Zamawiający wymaga dostarczenia kompletu niezbędnych przewodów zasilających o długości minimum 1,5m każdy, pozwalających na podłączenie oferowanego urządzenia z zasilaczem i zasilacza ze źródłem napięcia tj. listwą zasilającą 230V w standardzie EU

1.14. Do wszystkich oferowanych urządzeń należy dostarczyć przewody uziemiające o długości minimum 1,5 m wraz z odpowiednimi zakończeniami.

1.15. Zamawiający wymaga dostarczenia do każdego zasilacza jednej szyny DIN instalowanej w szafie RACK 19”
   a. szyna DIN musi umożliwiać instalację oferowanego urządzenia wraz z zasilaczem w standardzie DIN
   b. zestaw montażowy szyny DIN w szafie RACK musi mieć możliwość regulacji głębokości montażu, tak aby zainstalowane na niej urządzenia wraz z podłączonymi kablami/przewodami nie wystawały poza obręb uchwytów RACK 19”, tym samym umożliwiając zamkniecie drzwi szafy RACK.

1.16. System posiada podwójne zaciski do podania redundantnego zasilania napięciem stałym w zakresie 12-125 V DC.

1.17. Zużycie energii – maximum 20W

1.18. Brak wiatraków chłodzących zabudowanych w urządzeniu

2. Oczekiwane parametry wydajnościowe:
   2.1. W zakresie Firewall’a obsługa nie mniej niż 980 tys. jednoczesnych połączeń oraz 34 tys. nowych połączeń na sekundę.
   2.2. Przepustowość Stateful Firewall: nie mniej niż 8 Gbps dla pakietów 512 B.
   2.3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps.
   2.4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6.2 Gbps.
   2.5. 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 930 Mbps.
   2.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 490 Mbps.
   2.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 500 Mbps.
   2.8. Ilość wirtualnych systemów: 10

2. Dostawa systemu bezpieczeństwa

Zarządzanie systemem bezpieczeństwa

W ramach postępowania wymagane jest dostarczenie systemu centralnego zarządzania przystosowanego do współpracy z systemami bezpieczeństwa sieciowego NGFW (Next Generation

Firewall) zarówno oferowanych w ramach zapytania jak i posiadanych przez Zamawiającego FortiGate 601E. System musi być dostarczony w formie lokalnej maszyny z licencjami niewygasającymi (system musi działać bez wykupionego wsparcia).

Wymagania techniczne dla centralnego zarządzania:

1. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi, Amazon AWS, Citrix XenServer, Google Cloud Platform, Linux KVM, Microsoft Azure, Microsoft Hyper-V Server, OpenSource XenServer, Oracle Private Cloud
2. System musi umożliwiać zarządzenie co najmniej 30 systemami bezpieczeństwa NGFW tożsamymi z wirtualnymi instancjami firewall (określane jako domena/system).
3. System centralnego zarządzania musi posiadać mechanizm zarządzania zmianami konfiguracji bazujący na osobnych rolach administratorów wykonujących konfigurację oraz rolach administratorów zatwierdzających zmiany, a także mechanizm audytu oraz porównywania konfiguracji i powiadamiania za pośrednictwem poczty elektronicznej o konfiguracji oczekującej na zatwierdzenie.
4. System centralnego zarządzania musi dawać możliwość pełnej konfiguracji zarządzanych systemów NGFW ze wszystkimi ich funkcjami składowymi.
5. System centralnego zarządzania musi posiadać możliwość skonfigurowania godziny implementacji zmian (harmonogram instalowania zmian).
6. System centralnego zarządzania musi przechowywać i implementować polityki bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej.
7. System centralnego zarządzania musi umożliwiać sprawdzenie spójności polityki firewall (w tym m.in. wykrywanie zduplikowanych obiektów).
8. System musi umożliwiać tworzenie dynamicznych obiektów (np. adresów IP), których wartość może być definiowana niezależnie per każdy zarządzany system bezpieczeństwa NGFW.
9. System centralnego zarządzania musi umożliwiać wyszukiwanie obiektów po ich nazwach oraz filtrowanie widoku polityki firewall na podstawie wybranych atrybutów reguł firewall.
10. System centralnego zarządzania musi umożliwiać przypisywanie tych samych polityk firewall, profili bezpieczeństwa, polityk SD-WAN oraz wybranych ustawień systemowych do wielu zarządzanych systemów bezpieczeństwa NGFW.
11. System centralnego zarządzania musi umożliwiać tworzenie wielu wspólnych bloków polityk firewall, tzn. zestawów reguł firewall, które mogą być wykorzystane w wielu odrębnych politykach firewall przypisanych do różnych systemów bezpieczeństwa NGFW. Administrator musi mieć możliwość umieszczenia takiego bloku w wybranym przez siebie miejscu polityki firewall.
12. System centralnego zarządzania musi wersjonować konfiguracje w taki sposób, aby możliwe było odtworzenie wybranej konfiguracji zainstalowanej w przeszłości na systemie bezpieczeństwa NGFW a obecnie przechowywanej w systemie centralnego zarządzania jako historyczna.
13. System centralnego zarządzania musi umożliwiać zarządzanie wersjami firmware'u oraz zapewniać centralną aktualizację oprogramowania zarządzanych systemów NGFW. Administrator musi mieć możliwość określenia daty automatycznej aktualizacji oprogramowania dla wybranych zarządzanych systemów NGFW.
14. System centralnego zarządzania musi oferować możliwość aktualizacji baz sygnatur na zarządzanych systemach NGFW (zarządzane systemy NGFW nie muszą mieć dostępu do sieci Internet w celu aktualizacji swoich baz sygnatur).
15. System centralnego zarządzania musi umożliwiać podgląd licencji (wraz z terminem ich ważności) na zarządzanych systemach bezpieczeństwa NGFW.
16. System centralnego zarządzania musi umożliwiać zdalne wykonywanie skryptów na zarządzanych systemach bezpieczeństwa. W skryptach powinna być możliwość wykorzystania zmiennych,

których wartości przypisywane są niezależnie dla każdego zarządzanego systemu bezpieczeństwa NGFW.

17. System centralnego zarządzania musi umożliwiać monitoring zarządzanych systemów NGFW w zakresie m.in. aktualnych tablic routingu, funkcjonalności DHCP server, SD-WAN (opóźnienie, jitter, straty pakietów), statusu tuneli VPN IPSec.
18. System centralnego zarządzania musi zawierać informacje, kiedy po raz pierwszy i kiedy po raz ostatni ruch przetwarzany przez zarządzane systemy NGFW trafił w poszczególne reguły polityki firewall.
19. System centralnego zarządzania musi umożliwiać zarządzanie systemami NGFW znajdującymi się za NAT.
20. System centralnego zarządzania musi umożliwiać uruchamianie systemów NGFW bez wstępnej konfiguracji, zgodnie z przygotowanym wcześniej wzorcami konfiguracji (ang: *Zero Touch Provisioning*).
21. System musi optymalizować proces konfiguracji struktur VPN typu hub-and-spoke oraz full-mesh poprzez obiekty typu community/topologie VPN, umożliwiające proste dodawanie zarządzanych urządzeń w celu dołączenia ich do danej topologii VPN.
22. System zarządzania musi mieć możliwość pracy w trybie klastra niezawodnościowego, złożonego przynajmniej z dwóch elementów. Konfiguracja zarządzanych urządzeń musi być automatycznie synchronizowana pomiędzy wszystkimi elementami tego klastra.
23. System centralnego zarządzania musi mieć możliwość podziału na wirtualne systemy zarządzania (konteksty), które będą posiadały odrębne definicje obiektów. Musi istnieć możliwość przypisywania administratorom praw dostępu do wybranych wirtualnych systemów zarządzania.
24. System centralnego zarządzania musi umożliwiać pracę wielu administratorów jednocześnie System musi mieć możliwość blokady kontekstu (domeny administracyjnej), aby różni administratorzy nie mogli wykonywać w tym samym czasie zmian w tym samym kontekście. Administrator musi mieć także możliwość blokady tylko wybranej polityki firewall w obrębie całego kontekstu.
25. W przypadku pracy w trybie z kontekstami (domenami administracyjnymi) musi istnieć możliwość definiowania globalnych obiektów (np. adresów IP, portów TCP/UDP, profili bezpieczeństwa), które będą dostępne w wybranych kontekstach i gotowe do użycia np. w politykach firewall.
26. System musi pozwalać na włączanie lub wyłączanie widoczności w GUI systemu centralnego zarządzania wybranych elementów konfiguracji zarządzanych urządzeń.
27. System musi pozwalać na łatwą zamianę zarządzanego urządzenia NGFW, które uległo awarii, na nowe urządzenie tego samego modelu bez konieczności ponownego wykonywania jego pełnej konfiguracji czy ręcznego przenoszenia konfiguracji.
28. Wymaganiem jest, aby możliwe było wykorzystanie koordynat GPS z modemów urządzeń firewall do wyświetlania na mapie lokalizacji danego urządzenia.
29. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
30. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, TACACS+, PKI.
31. System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do wybranych elementów zarządzania oraz wybrania zarządzanych systemów dostępnych dla tego administratora.
32. Komunikacja pomiędzy systemem centralnego zarządzania a zarządzanymi systemami NGFW musi odbywać się w sposób szyfrowany.
33. System musi posiadać API, które umożliwia zarówno zarządzenie urządzeniami podłączonymi do systemu jak i samym systemem centralnego zarządzania.
34. System centralnego zarządzania musi mieć możliwość ustawienia języka polskiego lub angielskiego z poziomu graficznego interfejsu zarządzającego

Centralne uwierzytelnienie

Jako element oferowanego systemu bezpieczeństwa wymagane jest również dostarczenie systemu centralnego uwierzytelnienia w postaci maszyny wirtualnej spełniającego następujące wymagania:

1. Oferowane rozwiązanie musi pozwalać na centralne zarządzenie kontami użytkowników i ich uwierzytelnianiem. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie pochodziły od jednego producenta.
2. Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny, wzmocniony (hardenend) z punktu widzenia bezpieczeństwa.
3. System musi zapewniać obsługę nielimitowanej licencyjnie liczby wirtualnych procesorów, maksymalnie 1TB pamięci operacyjnej, 4 wirtualne interfejsy sieciowe oraz obsługę powierzchni dyskowej - minimum 16 TB.
4. Możliwość uruchomienia na platformach: Microsoft Hyper-V Server 2010, 2012 R2 oraz 2016, VMware ESXi / ESX 4 / 5 / 6 / 7, KVM, XEN oraz platformach chmury publicznej Microsoft Azure, Amazon AWS, Oracle OCI i AliCloud.
5. System powinien pozwalać na nie mniej niż:
   5.1. zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki, bez konieczności stosowania zewnętrznej konsoli zarządzającej
   5.2. pracę w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności – jeśli wymagana jest do tego licencja należy je dostarczyć
   5.3. odpytywanie o stan urządzenia w oparciu o protokół SNMP (v1, v2, v3) oraz wykorzystanie SNMP Trap celem monitorowania (nie mniej niż):
      5.3.1.obciążenia procesor(a/ów)
      5.3.2.wykorzystania pamięci
      5.3.3.obciążenia dysku
      5.3.4.zmiany adresu IP interfejsu
      5.3.5.informacji o osiąganiu granicznej liczby użytkowników
      5.3.6.informacji o osiąganiu granicznej liczby grup użytkowników
      5.3.7.przekroczeniu liczby uwierzytelnień
      5.3.8.przekroczeniu liczby błędnych uwierzytelnień
      5.3.9.zmiana stanu HA
   5.4. graficzną reprezentację statusu uwierzytelnień
   5.5. logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia i nazwy użytkownika:
      5.5.1.lokalnie
      5.5.2.zdalnie w oparciu o protokół syslog
   5.6. aktualizację systemu operacyjnego z poziomu graficznego interfejsu zarządzającego (GUI)
   5.7. tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI)
      5.7.1.również w oparciu o harmonogram w cyklu godzinowym, dziennym, tygodniowym lub miesięcznym wraz z określaniem godzin i minut
      5.7.2.rzeczona kopia bezpieczeństwa może również być również zapisywana przy pomocy protokołu FTP/SFTP
      5.7.3.szyfrowanie kopii bezpieczeństwa
   5.8. konfigurację captive portal
6. Celem realizacji funkcji uwierzytelniających, system powinien wspierać nie mniej niż:
   6.1. lokalną, wbudowaną bazę użytkowników wraz z możliwością wykonywania nie mniej niż następujących akcji na użytkowniku: tworzenie, przypisanie tokena i zarządzanie nim, blokowanie konta (locking), usuwanie

6.2. przechowywanie następujących informacji o użytkowniku: nazwa (username), imię/nazwisko, adres email, numer telefonu komórkowego, numer telefonu, adres, kraj, stan/województwo
6.3. możliwość przechowywania przynajmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników
6.4. możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV
6.5. konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:
6.5.1. poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych)
6.5.2. czasu życia hasła
6.5.3. możliwości ponownego użycia tych samych haseł
6.6. konfigurowalną politykę blokowania kont:
6.6.1. w oparciu o ilość nieudanych logowań
6.6.2. czas blokowania
6.6.3. okres nieaktywności po którym konto jest blokowane
6.7. możliwość odzyskiwania haseł:
6.7.1. z wykorzystaniem adresu email
6.7.2. z wykorzystaniem pytania pomocniczego
6.8. uruchomienie portalu do samodzielnej rejestracji użytkowników
6.8.1. opcjonalnie tworzenie ich kont może wymagać akceptacji administratora
6.8.2. wymagana jest również opcja tworzenie kont bez ingerencji administratora
6.9. obsługę protokołu RADIUS zgodną z RFC
6.9.1. wbudowany serwer RADIUS
6.9.2. konfiguracja serwera pozwala na ograniczenie dostępu tylko do wskazanych urządzeń NAS
6.9.3. integrację z zewnętrznymi serwerami RADIUS
6.9.4. możliwość importowania użytkowników RADIUS z zewnętrznego serwera LDAP
6.10. obsługę protokołu TACACS+
6.10.1. konfiguracja serwera pozwala na ograniczenie dostępu tylko dla wskazanych klientów
6.10.2. możliwość importowania klientów z pliku CSV oraz przy pomocy API
6.10.3. specyfikowanie listy dozwolonych/blokowanych poleceń powłoki i usług
6.11. obsługę protokołu LDAP
6.11.1. wbudowany serwer LDAP
6.11.2. możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP)
6.12. obsługę SAML - Identity Provider (IdP) proxy
6.13. realizacje funkcjonalności SSO (Single Sign On) w oparciu o:
6.13.1. integrację z Active Directory również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny
6.13.2. dedykowaną aplikację na stację robocze z systemem Windows
6.13.3. RADIUS
6.13.4. informacje uzyskiwane poprzez protokół syslog
6.13.5. dedykowany portal

7. Wymagania dla uwierzytelnienia dwuskładnikowego:
7.1. obsługę dla tokenów sprzętowych (hardware):
7.1.1. ich działanie musi być realizowane w oparciu o protokół OAuth wraz ze wsparciem dla TOTP oraz HOTP
7.1.2. wspomniane tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania
7.2. wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android. Dla tokenów na system iOS i Android wymaga się:
7.2.1. aktywacji z centralnego systemu uwierzytelniania (seed provisioning)

7.2.2. możliwości konfiguracji ilości generowanych cyfr (6 lub 8)
7.2.3. generowania kodu (cyfr) co 30 lub 60 sekund
7.2.4. możliwości dezaktywacji tokena oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne)
7.2.5. ochrony dostępu poprzez konfigurowalny kod PIN
7.2.6. aktywacji w oparciu o kod QR
7.2.7. możliwość przypisania własnego logotypu organizacji widocznego w aplikacji tokena mobilnego

7.3. możliwość dostarczenia kodu (wskazania tokena) poprzez:
7.3.1. email (wygaśnięcie kodu w czasie 10-3600 sekund)
7.3.2. SMS (wygaśnięcie kodu w czasie 10-3600 sekund)
7.3.2.1. konfiguracja bramki SMS w oparciu o HTTP/S i/lub SMTP

7.4. w przypadku tokenów programowych możliwość wykorzystania notyfikacji push przychodzących na urządzenie mobilne i zawierających szczegóły dotyczące żądania logowania (nazwa użytkownika, serwer/usługa docelowa, adres IP, data i godzina, rodzaj i wersja przeglądarki) w celu zaakceptowania ich jednym "kliknięciem"
7.5. możliwość integracji z logowaniem do systemu Windows
7.6. wsparcie dla API

8. System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki:
8.1. dla sieci bezprzewodowych wymagane są następujące protokoły:
8.1.1. PEAP
8.1.2. EAP-TTLS
8.1.3. EAP-TLS
8.1.4. EAP-GTC
8.2. wsparcie dla uwierzytelniania w oparciu o adres MAC (MAC based authentication)
8.3. zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTL, TLS EAP
8.4. możliwość samodzielnej rejestracji urządzeń przez użytkowników celem uwierzytelniania z wykorzystaniem certyfikatów
9. System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż:
9.1. własne, samodzielne CA (Certificate Authority)
9.2. CA pośredniczące (intermediary CA)
9.3. ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego
9.4. możliwość pobrania wygenerowanych certyfikatów
9.5. możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP
9.6. możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP
9.7. możliwość generowania certyfikatów typu wildcard
9.8. realizacja CRL (Certificate Revocation List)
9.9. wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560)
10. System musi obsługiwać co najmniej uwierzytelnianie dla 1000 użytkowników
11. System musi być kompatybilny w sposób przygotowany przez producenta z posiadanym przez Zamawiającego tokenami FortiTokenMobile w ilości 600.

Wymagania dla gwarancji i wsparcia technicznego oraz czas trwania

Dostawa gotowych komponentów

Dostarczone rozwiązanie Firewall oraz system zarzadzania, centralne uwierzytelnianie w tym wszystkie inne komponenty wchodzące w zakres wyżej wymienionych muszą zostać objęte oficjalnym serwisem producenta, w wymiarze 24x7, na okres min. 12 miesięcy w reżimie NBD. Jeżeli do realizacji wymaganych funkcjonalności potrzebę są licencje – zamawiający wymaga ich dostarczenia na okres minimum tożsamy z okresem wsparcia – tj. na okres min. 12 miesięcy.

Na wykonane prace w ramach umowy

Na wszystkie prace wykonane przez Wykonawcę w okresie 12 miesięcy od odbioru Zamawiający może przekazać zgłoszenie które Wykonawca musi rozwiązać w ciągu 2 dni roboczych.

Dodatkowe informacje

Gwarancja na dostarczony sprzęt, oprogramowanie i wszelkie prace biegnie od momentu podpisania protokołu odbioru bez uwag przez okres 12 miesięcy.

3. Wdrożenie

Wymagania dla usług wdrożeniowych

Zamawiający oczekuje od oferenta wdrożenia oferowanego rozwiązania w zakresie:

1. Przygotowanie projektu technicznego (maksymalnie 10 dni roboczych od podpisania umowy)
2. Przygotowanie harmonogramu wdrożenia (maksymalnie 7 dni roboczych od podpisania umowy)
3. System centralnego zarządzania:
    a. Instalacja i konfiguracja wstępna
    b. Konfiguracja uwierzytelnienia i uprawnień
    c. Podłączenie wszystkich urządzeń do zarządzania
    d. Weryfikacja prawidłowej komunikacji z urządzeniami
    e. Przygotowanie konfiguracji startowych dla urządzeń, ustawienie regularnej kopii konfiguracji
    f. Konfiguracja działania systemu zgodna z dobrymi praktykami
    g. Przygotowanie 2 ekranów kontrolnych (dashboard)
    h. Przygotowanie 10 raportów
    i. Instruktaż z obsługi systemu dla pracowników zamawiającego w zakresie 1 dnia roboczego.
    j. Testy techniczne systemu
4. System centralnego uwierzytelniania:
    a. Instalacja i konfiguracja wstępna
    b. Migracja tokenów z obecnego systemu
    c. Wstępna konfiguracja dla tokenów sprzętowych
    d. Ustawienie regularnej kopii konfiguracji
    e. Konfiguracja działania systemu zgodna z dobrymi praktykami

f. Instruktaż z obsługi systemu dla pracowników zamawiającego w zakresie 1 dnia roboczego.
g. Testy techniczne systemu

5. Urządzenia firewall:
    a. Aktualizacja oprogramowania
    b. Przygotowanie konfiguracji startowej
    c. Uruchomienie i przetestowanie komunikacji modemów LTE
    d. Instruktaż z podstawowych zadań konfiguracyjnych i operacyjnych dla pracowników zamawiającego w zakresie 1 dnia roboczego.
    e. Testy techniczne systemu
6. Wykonanie dokumentacji powdrożeniowej
    a. Kopia wszystkich konfiguracji
    b. Dokumentacja wykonanych prac w postaci dokumentu word
    c. Zalecenia powdrożeniowe
    d. Procedura zgłaszania problemów technicznych
    e. Potwierdzenie wykonanych testów odbioru systemu.

Dodatkowe wymagania:

Bieżące wsparcie techniczne

a. 160 godzin roboczych wsparcia technicznego przeznaczone na konsultacje i ustalanie zmian konfiguracyjnych.
b. Bieżące wsparcie techniczne dla wykrytych problemów technicznych
c. Pośredniczenie w zgłaszaniu problemów technicznych do serwisu producenta.

Zespół wdrożeniowy

Zamawiający wymaga od Wykonawcy dysponowaniem co najmniej 1 inżynierem z aktualnym certyfikatem na poziomie min. NSE5 lub równoważnym oraz 1 inżynierem z aktualnym certyfikatem na poziomie min. NSE7 lub równoważnym. Wymieniony personel musi być bezpośrednio zaangażowany w realizację zamówienia.