SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – PAKIET NR 3

Wymagania Ogólne

1. Muszą to być specjalizowane urządzenie sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako klaster wysokiej dostępności (HA) w trybach Active/Standby, Active/Active.
2. Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta. Producent oferowanego rozwiązania musi być obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders przynajmniej od 2 lat.
3. Urządzenia muszą umożliwiać działanie w następujących trybach pracy:
    a. rutera (tzn. w warstwie 3 modelu OSI),
    b. mostu (tzn. w warstwie 2 modelu OSI),
    c. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; Musi pracować w trybie przezroczystego łączenia interfejsów w pary.).
    d. w trybie pasywnego nasłuchu (sniffer/tap).
4. System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
5. Urządzenia firewall muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu od zasobów służących do zarządzania urządzeniem.
6. Urządzenie musi posiadać dedykowane zasoby/rdzenie procesora/procesorów do funkcji zarządzania urządzeniem lub możliwość ustawienia dedykowanych zasobów/rdzeni procesora/procesorów do funkcji zarządzania urządzeniem.
7. Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.
8. Urządzenia firewall muszą wspierać protokół LACP.
9. Urządzenia firewall muszą zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
10. Urządzenia firewall muszą działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.
11. Polityka zabezpieczeń firewall musi uwzględniać
    a. adresy IP źródłowe i docelowe,
    b. protokoły i usługi sieciowe,
    c. aplikacje,
    d. kategorie URL,
    e. użytkowników aplikacji i grupy,
    f. reakcje zabezpieczeń,
    g. logowanie zdarzeń (początek i koniec sesji)
    h. strefa wejściowa i wyjściowa
12. Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65535 dostępnych

portach. Przy tym wydajność kontroli firewalla stanowego i kontroli aplikacji całego ruchu nie może być mniejsza, niż wskazano w wymaganiach wydajnościowych urządzeń.
Urządzenie musi wykrywać co najmniej 3700 predefiniowanych aplikacji wspieranych przez producenta (takich jak DNS over HTTPS, Telegram, Skype, Tor, BitTorrent, MQTT, Modbus, DNP3, Siemens S7) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.

13. Urządzenia firewall muszą pozwalać na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.
14. Urządzenia firewall muszą zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.
15. Urządzenia firewall muszą być wyposażone w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy dostarczyć odpowiednie dla minimum 30 administratorów.
16. Dostęp do urządzeń i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
17. Urządzenia firewall muszą umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż:
    a. baza lokalna,
    b. serwer Radius,
    c. serwer TACACS+,
    d. serwer AD/LDAP.

    Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH a dla dostępu GUI za pomocą certyfikatów kryptograficznych.
18. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
    a. Active Directory,
    b. Terminal Services
19. Polityka kontroli dostępu (urządzeń firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości musi odbywać się również transparentnie.
20. Urządzenia firewall muszą pozwalać na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL.
21. Urządzenie musi dostarczać predefiniowane przez producenta raporty standardowe jak i możliwość tworzenia raportów niestandardowych. Na urządzeniu musi być również dostępne

tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu.

22. Urządzenie musi pozwalać na zapisanie raportów na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
23. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
    a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
    b. API
24. Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESX i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można potem wykorzystywać w polityce bezpieczeństwa urządzeń.
25. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.
26. Urządzenia firewall muszą obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
27. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
28. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami NAT.
29. Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju.
30. Urządzenia firewall muszą obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
31. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa.
32. Wykonywanie operacji deszyfrowanie ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji. Musi zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.
33. Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL.
34. Dla deszyfrowania ruchu TLS 1.3 wymagane jest wsparcie dla X25519, X448 oraz minimum dla zestawów protokołów: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384 oraz TLS_CHACHA20_POLY1305_SHA256.
35. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
36. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) i ustawiania dla aplikacji priorytetu oraz pasma.
37. Urządzenia firewall muszą umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. routing-based VPN).

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – PAKIET NR 3

38. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
39. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
40. Urządzenia firewall muszą zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tuneli SSH.
41. Urządzenia firewall muszą posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
42. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur albo powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.
43. Urządzenia firewall muszą posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.
44. Urządzenia firewall muszą posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół minimum: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż raz na 48 godzin i pochodzić od tego samego producenta co firewall.
45. Urządzenia firewall muszą posiadać funkcję anty-spyware. Baza sygnatur musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.
46. Rozwiązanie musi posiadać możliwość analizy nieznanej komunikacji C2 (command-and-control) oraz spyware w oparciu o nauczanie maszynowe realizowane w czasie rzeczywistym, przy czym:
    a. musi być możliwe jest blokowanie wykrytej komunikacji C2 w czasie rzeczywistym,
    b. powyższe musi być możliwe minimum dla ruchu typu: HTTP, HTTP/2, SSL oraz niezidentyfikowanych przez urządzenie aplikacji w ruchu TCP i UDP.
47. Urządzenia firewall muszą posiadać funkcję filtrowania URL.
48. Funkcja filtrowania URL musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
49. Rozwiązanie musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania kategorii URL.
50. Urządzenia firewall muszą umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „SandBox” plików wykonywalnych PE i DLL przechodzących przez firewall. Systemy sandbox, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików, adresów IP, DNS i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik. Maksymalny interwał aktualizacji sygnatur 48 godzin.
51. System zabezpieczeń NGFW musi dodatkowo oferować możliwość identyfikacji w ruchu sieciowym i przesyłania do zintegrowanej usługi analizy dynamicznej (tzw. „sandbox”) plików następujących typów: wykonywalnych (PE), Microsoft Office, Adobe flash / PDF, archiwa: JAR, RAR, 7-ZIP, Android APK, Mac OSX, skrypty: BAT, JScript, PowerShell, VBS, Perl i Python. W przypadku potwierdzenia nieznanego ataku (tzw. “zero-day”), musi następować automatyczna aktualizacja systemu firewall nowymi sygnaturami opisującymi wykryte pliki malware lub ich

zidentyfikowane złośliwe zachowania (np. wzorce komunikacji zwrotnej) w wyniku przeprowadzonej analizy.

52. Uruchomienie ochrony typu “sandbox” dla systemu zabezpieczeń NGFW musi być możliwe w następujących trybach:
    a. Subskrypcji - bez dokupowania jakichkolwiek komponentów sprzętowych wyłącznie w oparciu o usługę chmurową producenta rozwiązania (bez wersji “advanced wildfire” można dodać: uruchamianą na terenie EU)
    b. Prywatnym - po zakupieniu dodatkowego urządzenia do analizy lokalnej
    c. Hybrydowym - z wykorzystaniem zarówno subskrypcji i po zakupieniu urządzenia do analizy lokalnej
53. W każdym z powyższych trybów, administrator systemu NGFW musi mieć możliwość konfiguracji rodzaju pliku, kontekstu użytej aplikacji, kierunku transmisji (wysyłanie / odbieranie) i miejsca analizy (chmura / urządzenie lokalne) dla celów definicji ruchu i klasyfikacji obiektów do analizy typu „sandbox”.
54. Zintegrowana z rozwiązaniem NGFW subskrypcja “sandbox” powinna mieć udokumentowane wsparcie producenta dla najnowszych technik analizy złośliwego oprogramowania:
    a. wykorzystanie własnego, utwardzonego hypervisor-a, względem potencjalnych metod rozpoznawania generycznego środowiska wirtualnego przez malware,
    b. automatyczne rozpakowanie malware-u zaciemnionego metodami kompresji (tzw. packer-ów) celem pełnej widoczności zachowania jego kodu,
    c. emulacja zależności wymaganych przez potencjalnie złośliwe oprogramowanie do jego pełnego uruchomienia w środowisku piaskownicy,
    d. tworzenie zrzutów pamięci dla potencjalnie złośliwych zachowań podczas wykonywania kodu jako sposobu monitorowania środowiska piaskownicy i ich uwzględnienia w werdykcie końcowym**.**
55. Urządzenia firewall muszą umożliwiać zabezpieczenie działania protokołu DNS poprzez procesowanie zapytań DNS w celu wykrywania i blokowania: zagrożeń, wycieku danych (exfiltracja), tunelowania DNS. Urządzenia muszą posiadać ciągły (on-line) dostęp do centralnego repozytorium zagrożeń DNS, który będzie wykorzystywany w procesie decyzyjnym funkcjonalności.
56. W przypadku gdy jakakolwiek funkcjonalność lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres 60 miesięcy od daty odbioru sprzętu.
57. Wsparcie serwisowe (techniczne) i gwarancja dla systemu (zwana dalej wsparciem) będzie świadczone przez producenta lub autoryzowane przez producenta centrum serwisowe, niezależne od Wykonawcy, realizowane we współpracy z producentem, przez okres 60 miesięcy od daty odbioru sprzętu.

PARAMETRY SPRZĘTOWE

1. Cechy urządzenia (parametry minimalne, muszą być spełnione dla każdego z dostarczanych urządzeń firewall):
    a. Wysokość maksymalnie 1U wraz z zestawem montażowym do szafy RACK 19”,
    b. Możliwość podłączenia redundantnego źródła zasilania,

   c. 8 portów 10/100/1000 Mbps Ethernet RJ45.
2. Rozwiązanie musi muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45, w co najmniej jeden dedykowany port zarządzający realizowany jako port 10/100/1000 Mbps Ethernet lub jako port SFP z wkładką 1000BASE-T.
3. Obsługa (parametry minimalne, parametry wydajnościowe muszą być spełnione dla każdego z dostarczanych urządzeń firewall):
   a. 2,2 Gbps przepustowości Firewall/kontroli aplikacji,
   b. 0,9 Gbps przepustowości Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware,
   c. 200 000 jednoczesnych sesji,
   d. 37 000 nowych połączeń na sekundę,
   e. Lokalnej przestrzeni na system operacyjny i logi co najmniej o pojemności minimum 128GB.
4. Jako scenariusz firewall/kontroli aplikacji Zamawiający rozumie, iż rozwiązanie pozwoli na:
   a. wykrycie aplikacji,
   b. przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.
5. Jako scenariusz firewall/IPS/antywirus/kontroli aplikacji/antymalware Zamawiający rozumie, iż rozwiązanie pozwoli na:
   a. wykrycie aplikacji,
   b. przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych, inspekcje IPS, antywirus, antyspyware.
6. Zakres kontroli musi też obejmować przesyłanie plików do sandboxa lokalnego i chmurowego w tym przechwytywanie i blokowanie plików określonego typu.
7. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla rozwiązania sygnaturami IPS oraz z wszystkimi funkcjami dostępnymi w rozwiązaniu dla silników antywirus i antyspyware/antymalware.
8. Inspekcjom bezpieczeństwa musi podlegać cały ruch – sprawdzeniu musi podlegać każdy bajt danych przesyłany przez rozwiązanie.
9. Zamawiający wymaga, aby podana została przepustowość urządzenia dla pełnego zakresu ochrony oferowanego przez rozwiązanie – jeżeli rozwiązanie pozwala na pracę w wielu trybach, to należy podać przepustowość dla trybu z największą liczbą dostępnych inspekcji dla silników IPS, antywirus, antymalware/antyspyware.
10. Rozwiązanie musi spełniać co najmniej następujące parametry wydajnościowe odnośnie funkcjonalności site-to-site VPN:
    a. minimum 1,7 Gbps dla IPSEC VPN
    b. minimum 2800 tuneli IPSEC VPN (site-to-site).
11. Rozwiązanie musi spełniać co najmniej następujące parametry wydajnościowe odnośnie funkcjonalności remote access VPN:
    a. minimum 1000 tuneli VPN Remote Access z wykorzystaniem klienta VPN.

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – PAKIET NR 3

Oprogramowanie klienta VPN musi być objęte wsparciem producenta.

b. minimum 100 tuneli tzw. Clientless VPN - bez konieczności zastosowania klienta

12. Rozwiązanie musi obsługiwać nie mniej niż 3 wirtualnych routerów posiadających odrębne tabele routingu.
13. Musi mieć możliwość rozbudowy do przynajmniej 2 wirtualnych instancji firewall (określanych jako kontekst/domena/system). Każda z instancji musi pozwalać na konfigurację niezależnych oraz odrębnych od innych instancji – polityk bezpieczeństwa (co najmniej dla IPS, AV i współpracy z sandboxem), tablicy routingu oraz realizacji zdalnego dostępu.

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – PAKIET NR 3

OCENA TECHNICZNA

Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:

1. **Cena oferty brutto - 60 %**
2. **Ocena techniczna - 40 %**

Ocena techniczna = ilość przydzielonych punktów x waga kryterium (**40 %**)

Za najkorzystniejszą zostanie wybrana oferta z największą ilością punktów w sumie kryteriów ceny oferty brutto i oceny technicznej.

Ocena techniczna - 40 %

Zamawiający przydzieli punkty za to kryterium na podstawie informacji podanej w Formularzu Oferty na podstawie oceny technicznej przedstawionej w poniżej:

1) Ochrona z wykorzystaniem mechanizmów MACHINE LEARNING – 15 punktów

Urządzenie NGFW musi pozwalać na blokowanie zagrożeń za pomocą algorytmów uczenia maszynowego (ML) aktualizowanego dynamicznie przez producenta. Wykrywanie i blokowanie złośliwych treści musi odbywać się lokalnie na urządzeniu, jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antywirusowych. Funkcja wykrywania zagrożeń z wykorzystaniem mechanizmów ML musi być dostępna co najmniej dla:

a. Złośliwych plików wykonywalnych (PE), ELF, Ms Office;
b. Złośliwych skryptów PowerShell;

Wykonawca, który deklaruje spełnienie kryterium „Urządzenie NGFW musi pozwalać na blokowanie zagrożeń za pomocą algorytmów uczenia maszynowego (ML) aktualizowanego dynamicznie przez producenta. Wykrywanie i blokowanie złośliwych treści musi odbywać się lokalnie na urządzeniu, jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antywirusowych.

2) Koncept konfiguracji kandydackiej – 10 punktów

Urządzenie musi posiadać koncept konfiguracji kandydackiej (na poziomie API, GUI oraz CLI), którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.
W tym:

a. Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian, których są autorami.
b. Możliwość blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji

3) Ochrona przed próbą wyłudzenia poświadczeń - 5 punktów

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – PAKIET NR 3

Możliwość zdefiniowania stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia Active Directory. W przypadku próby wysłania poświadczeń Active Directory do niezaufanej strony lub serwisu administrator może zdefiniować odpowiednią politykę blokującą dla takiego zdarzenia.

4) Weryfikacja nowo pobranych aktualizacji sygnatur - 10 punktów

Urządzenie musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur aplikacyjnych (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa – funkcja ta musi być wbudowana w firewall i nie może wymagać korzystania z rozwiązań firm trzecich.

Warunki serwisu technicznego i procedura zgłoszeń

Wsparcie techniczne musi być świadczone w języku polskim przez producenta lub oficjalnego partnera producenta urządzeń w zakresie świadczenia pomocy serwisowej.

Wsparcie techniczne musi być świadczone **przez okres 60 miesięcy** . W ramach świadczenia gwarancyjnego, w wypadku wystąpienia awarii zamawiający otrzyma część zamienną/urządzenie objęte gwarancją w trybie następnego dnia roboczego. Wraz z dostarczonym sprzętem będzie świadczony dostęp do strony pomocy technicznej producenta oraz możliwość pobierania aktualizacji oprogramowania związanego z oferowanym sprzętem.