Załącznik nr 3 do projektu umowy

Szczegółowy Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest rozbudowa systemu zabezpieczeń firewall w segmencie LAN przez (NFV/VM wirtualizację funkcji sieciowych realizowana na systemie Vmware) polegająca na wymianie urządzeń i modernizacji posiadanego przez Zamawiającego środowiska do zarządzania urządzeniami bezpieczeństwa NGFW (Firewall nowej generacji).

W ramach postępowania Zamawiający wymaga również przedłużenia licencji wraz ze wsparciem dla urządzeń zgodnie z poniższą tabelą nr 1 na okres 1 roku.
Zamawiający jest w posiadaniu:
- Model PA-3020 Serial #001801015631
- Model PA-3020 Serial #01801015652
- Model Panorama Serial # 000702883886

Tabela nr 1

Lp	Kod	Opis	Ilość/Host	Okres
1	PAN-PA-3020-GP-HA2-R	GlobalProtect subscription renewal for devices in HA pair, PA-3020	2	1 rok
2	PAN-PA-3020-URL4-HA2-R	PANDB URL filtering subscription renewal for devices in HA pair, PA-3020	2	1 rok
3	PAN-PA-3020-TP-HA2-R	Threat prevention subscription renewal for devices in HA pair, PA-3020	2	1 rok
4	PAN-SVC-BKLN-3020-R	Partner enabled premium support year 1 renewal, PA-3020	2	1 rok
5	PAN-SVC-BKLN-PRA-25-R	Partner enabled premium support renewal, Panorama 25 devices	2	1 rok
6	PAN-PA-3020-WF-HA2-R	WildFire subscription renewal for devices in HA pair, PA-3020	2	1 rok

oraz

1. Przeprowadzenia aktualizacji sytemu do rekomendowanej wersji urządzeń PAN-PA-3020 pracujących w klastrze HA.
2. Sprawdzenia poprawności działania systemu.

Wdrożenie:

1) Instalacja fizyczna platformy NFV.
2) Instalacja Hypervisora VMware na platformie NFV.
3) Podłączenie platformy NFV całości do infrastruktury Zamawiającego (przełączniki/routery).
4) Instalacja klastra systemu zabezpieczeń firewall (NGFW) na platformie NFV.
5) Konfiguracja systemu zabezpieczeń firewall (NGFW) zgodnie z wymaganiami Zamawiającego.
6) Integracja systemu zabezpieczeń firewall (NGFW) z posiadanym przez Zamawiającego systemem Palo Alto Panorama.
7) Przeniesienie pełnej konfiguracji ze starego systemu z Cisco ASA 5510 v.8.2 i 8.0 (dla połączeń przewodowych i bezprzewodowych w sieci LAN) na nowe urządzenia.

8) Przeniesienie ma obejmować między innymi:
   - reguły bezpieczeństwa
   - reguły translacji NAT
   - trasy routingu
   - ustawienia interfejsów sieciowych (fizycznych i wirtualnych)
   - oraz innych elementów konfiguracji (obiektów, grup obiektów itp.
9) Sprawdzenie poprawności działania systemu i ruchu sieciowego opartego na przeniesionej konfiguracji.
10) Wykonanie dokumentacji powdrożeniowej.
11) Usługę wsparcia po wdrożeniowego w ilości 4 dni roboczych, świadczonych na miejscu w godzinach 8-16.

Dodatkowe wymagania odnośnie urządzeń:

- Oferowane urządzenia muszą być fabrycznie nowe i pochodzić z legalnego kanału sprzedaży producenta na rynek polski.
- Oferowane urządzenie muszą być nie starsze niż 6 miesięcy od ogłoszenia przetargu.
- Urządzenie musi posiadać co najmniej 36 miesięczną gwarancję na hardware i software systemowy.
- Urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO 9001:2000 lub normą równoważną.
- Urządzenie i jego komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
- Urządzenie musi być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
- Do urządzenia musi być dostarczony komplet standardowej dokumentacji w formie papierowej lub elektronicznej. Ewentualnie musi być możliwość uzyskania dostępu do takiej dokumentacji w postaci elektronicznej.
- Urządzenie musi współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
- Urządzenie muszą być zainstalowane w standardowej szafie rack w siedzibie Zamawiającego.

Szczegółowe wymagania odnośnie urządzeń:

Serwer/Platforma NFV (wirtualizacja funkcji sieciowych) – 2 szt.

1) Obudowa
   a. Obudowa ze wszystkimi komponentami umożliwiająca montaż w standardowej szafie typu rack
   b. Wysokość maksymalnie 2U
   c. Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack
2) Płyta główna
   a. Dwuprocesorowa, z możliwością instalacji procesorów min. 28-rdzeniowych
   b. Płyta musi obsługiwać SR-IOV oraz VT-D i sprzętową wirtualizację
   c. Możliwość instalacji minimum 3 złącz PCI Express (1 CPU) oraz możliwość rozbudowy do obsługi 7 złącz PCI Express (po dodaniu drugiego CPU) za pomocą tzw. riser-cards. Jedno ze złącz PCI Express może być realizowane

poprzez tzw. slot klasy LOM o ile wspiera instalację kart sieciowych 4 portowych 10Gbit/s. Przynajmniej jeden ze slotów PCI musi być typu Low-Profile

   d. Możliwość integracji dedykowanej, szybkiej wewnętrznej pamięci SSD przeznaczonej dla wirtualizatora (niezależne od dysków twardych) – musi istnieć możliwość instalacji dwóch pamięci pracujących jako macierz RAID1 (mirror); Pamięć ta musi być zgodna (poziom sterowników i HCL) z oprogramowaniem VMware vSphere 6.x i nowszym

3) Procesory
   a. Zainstalowany jeden procesor (CPU) w architekturze x86 posiadający minimum 8 rdzenie. Procesor musi posiadać minimum 11MB pamięci SmartCache oraz wspierać pamięci typu DDR4. Pojedynczy rdzeń nie może być taktowany (nominalnie) mniej niż 3.2GHz oraz nie mniej niż 4.0GHz (tryb Turbo). Procesor musi wspierać instrukcje typu Advanced Vector Extensions 512 (AVX-512). Procesor musi wspierać technologię Hyper-Threading.
4) RAM – Pamięć Operacyjna
   a. Zainstalowane min. 32 GB pamięci RAM typu DDR4
   b. Wsparcie dla technologii zabezpieczania pamięci Advanced ECC
   c. 24 gniazda pamięci RAM na płycie głównej, obsługa minimum 2TB pamięci RAM DDR4
5) HDD – Dyski twarde
   a. Minimum 2 dyski SSD – pojemność minimalna każdego dysków 240GB. Parametr DWPD dla dysku nie gorszy niż 0.5.
   b. Sprzętowy kontroler RAID – obsługa RAID 1 (Mirror). Kontroler musi posiadać pamięć cache minimum 1GB z zabezpieczeniem FBWC lub BWBC
6) Ethernet/FC
   a. Minimum 4 porty 10GE SFP+ bazujące na chipset'cie 82599 (X520) lub X710. Porty muszą wspierać SR-IOV. W portach muszą być zainstalowane wkładki 10GBase-SR
   b. Minimum 2 porty 1GE RJ45 10/100/1000
7) Porty
   a. zintegrowana karta graficzna
   b. 2 x min. USB 3.0 zewnętrzne z tyłu obudowy
   c. 1 x min. USB 3.0 zewnętrzne z przodu obudowy
   d. 1 x min. USB 2.0 zewnętrzne z przodu obudowy
   e. 1 x VGA (DB15) zewnętrzne z tyłu obudowy
   f. Zamawiający nie dopuszcza aby zewnętrzne porty były rozszywane za pomocą specjalistycznych, niestandardowych kabli
8) Zarządzanie
   a. Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o następujących funkcjonalnościach:
   b. Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera
   c. Dedykowana karta LAN 1GE RJ45 10/100/1000 (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym
   d. Dostęp poprzez przeglądarkę Web (także SSL, SSH)
   e. Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii
   f. Zarządzanie alarmami (zdarzenia poprzez SNMP)

g. Możliwość przejęcia konsoli tekstowej
h. Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM). Przekierowanie nie może wymagać JAVA.
i. Karta zarządzająca musi wspierać monitoring karty RAID (logiczne volumeny, fizyczne dyski, grupy RAID) jeśli takowa jest zainstalowana w serwerze
j. Jeśli wymagane są licencje dla wyżej opisanych funkcjonalności – należy je dostarczyć wraz z serwerem

9) Zasilanie
   a. Zainstalowane dwa redundantne zasilacze hot-plug o mocy minimalnej 500W każdy (jednak nie większej niż 1400W)
10) Wspierane OS
   a. VMWare ESXi 6.x/7.x – wymagana certyfikacja VMware.
11) Gwarancja
   a. 36 miesięcy na urządzenia fizyczne.
   b. bezpłatne aktualizacje firmware.
   c. wymianę uszkodzonego komponentu w siedzibie Zamawiającego lub przesłanie nowego komponentu w miejsce uszkodzonego następnego dnia roboczego od uznania awarii.
   d. dostęp do bazy wiedzy producenta
   e. dostęp do TAC producenta (otwieranie tzw. case'ów) – brak limitu otwierania zgłoszeń w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware
   f. realizacja serwisu w porozumieniu z producentem – tzw. Partner Support lub bezpośrednio przez producenta. W przypadku gwarancji Partner Support podmiot realizujący wsparcie musi posiadać certyfikat certyfikowanego partnera serwisowego wydany przez producenta urządzeń

System zabezpieczeń firewall (NGFW) – 2 szt.

1) System zabezpieczeń firewall musi być dostarczony w formie maszyny wirtualnej. W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość oprogramowania musi być dostarczana i wspierana przez jednego producenta.
2) System zabezpieczeń firewall musi być w pełni zarządzany i kontrolowany przez posiadany przez Zamawiającego system **Palo Alto Networks Panorama**. W ramach zarządzania reguły firewall w wzorcach (Templates) muszą być obsługiwane przez dostarczany system zabezpieczeń firewall.
3) System zabezpieczeń firewall zostanie zainstalowany na dostarczanych serwerach/platformie NFV.
4) System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 8 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 4 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, Threat Protection/Prevention, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 2 000 000 jednoczesnych połączeń. Dla opisanych parametrów system nie może wymagać więcej zasobów sprzętowych niż 8 vCPU taktowane na poziomie nie mniejszym niż 3.5GHz per fizyczny CPU (bez funkcji akcelerujących typu Turbo).
5) System zabezpieczeń firewall musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym (bridge) oraz w trybie pasywnego nasłuchu (sniffer/tap). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA.
6) Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
7) System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN. System musi potrafić używać fizycznych portów platformy NFV z wykorzystaniem SR-IOV i odpowiednim wsparciem Hypervisora.
8) System zabezpieczeń firewall musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.
9) System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
10) Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).
11) System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.

12) System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
13) 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 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 4 Gbit/s.
14) Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).
15) Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
16) Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
17) System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.
18) System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
19) System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
20) System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, pdf, pgp, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
21) System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
22) System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.
23) System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
24) System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie

i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.

25) System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
26) System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
27) System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
28) System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (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, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
29) System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.
30) System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.
31) Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.
32) System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL.
33) System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
34) System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
35) System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
36) System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów,

poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

37) System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
38) System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
39) System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
40) System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
41) System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
42) System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
43) System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
44) System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
45) System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
46) System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
47) System zabezpieczeń firewall musi ochraniać sieć przed tunelowaniem ruchu poprzez protokół DNS.
48) System zabezpieczeń firewall musi ochraniać sieć przed złośliwym oprogramowaniem (malware) wykorzystującym atak Domain Generation Algorithm (DGA).
49) System musi umożliwiać wykrywanie domen DGA i ruchu tunelowanego poprzez protokół DNS.
50) System zabezpieczeń firewall musi ochraniać sieć przed złośliwymi domenami.

51) System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
52) System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany.
53) System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
54) System zabezpieczeń firewall musi posiadać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 2 Gbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.
55) Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".
56) Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box".
57) System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.
58) System zabezpieczeń firewall musi wykonywać 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. Dodatkowo translacja NAT musi działać dla interfejsów transparentnych (L2 ISO/OSI bridge).
59) System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
60) System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
61) System zabezpieczeń firewall musi 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 rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.
62) System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.

63) System zabezpieczeń firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną). Musi istnieć możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci.
64) System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0.
65) System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
66) System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
67) System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
68) System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.
69) Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
70) System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej 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.
71) System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.
72) System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
73) System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
74) Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.

75) System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.
76) System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
77) System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 60 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
78) System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
79) System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
80) System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.
81) System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
82) System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
83) System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.
84) System zabezpieczeń firewall musi pracować jako koncentrator usługi SD-WAN, gdzie urządzeniami wyniesionymi są inne urządzenia/maszyny VM tego samego producenta co dostarczane rozwiązanie NGFW.
85) System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
86) System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
87) System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
88) System zabezpieczeń firewall musi posiadać możliwość budowy klastra wysokiej dostępności z nie mniej niż 14 firewall'i tego samego typu.
89) Pomoc techniczna w języku polskim.
90) Do wszystkich modułów bezpieczeństwa (AV, IPS, AS, URL, blokowanie plików, Sandbox) Zamawiający wymaga licencji na okres 1 roku.
91) Licencja bezterminowa na dostęp pełny do urządzenia i przesyłania ruchu sieciowego.
92) Wymagane jest, aby NGFW był objęty min. gwarancją przez okres co najmniej 12 miesięcy z zachowaniem poniższych warunków:
    a. bezpłatne aktualizacje firmware.
    b. bezpłatny re-host licencji w przypadku reinstalacji maszyny VM.
    c. dostęp do bazy wiedzy producenta.

d. dostęp do TAC producenta (otwieranie tzw. case'ów) – brak limitu otwierania zgłoszeń w przypadku podejrzenia możliwości błędu w oprogramowaniu.
e. realizacja serwisu w porozumieniu z producentem – tzw. Partner Support. Podmiot realizujący wsparcie musi posiadać certyfikat certyfikowanego partnera serwisowego wydany przez producenta urządzeń.
f. serwis musi być świadczony w języku Polskim.