Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

Zwiększenie wydajności systemów bezpieczeństwa Next Generation Firewall

I. Przedmiot zamówienia

W związku z koniecznością zwiększenia wydajności systemów bezpieczeństwa Next Generation Firewall użytkowanych w Urzędzie Miasta Gorzowa Wlkp., Zamawiający zamierza rozbudować posiadany system Palo Alto Networks o dwa kolejne urządzenia pracujące w klastrze wysokiej dostępności wraz z usługami Advanced Threat Prevention (ATP), Advanced URL Filtering (ADVURL) i Global Protect (GP).

Zamawiający użytkuje klaster wysokiej dostępności urządzeń Next Generation Firewall firmy Palo Alto Networks w poniższej konfiguracji:

P/N	opis	ilość
PAN-PA-3220	Palo Alto Networks PA-3220 with redundant AC power supplies	2
PAN-PA-3220-ATP-3YR-HA2	Advanced Threat Prevention subscription 3 year term for device in an HA pair, PA-3220	2
PAN-PA-3220-GP-3YR-HA2	GlobalProtect subscription 3 year term for device in an HA pair, PA-3220	2
PAN-PA-3220-ADVURL-3YR-HA2	Advanced URL Filtering Subscription, 3-year, PA-3220 HA Pair	2
PAN-SVC-BKLN-3220-3YR	Partner enabled premium support 3-year term, PA-3220	2

Powyższe urządzenia Palo Alto Networks są skonfigurowana w następujący sposób:

a) Fizycznie PA połączone są w pare HA, posiadają zestawione łączą do:
   - sieć WAN (uruchomiony protokół BGP) 2x 10G - dwa nie zależne łącza
   - Sieć DMZ - 2x10G LACP do urządzeń cisco i brocade ICX (około 20 sieci DMZ)
   - Sieć LAN - 2x10G LACP (uruchomiony protokół ospfv2) - cluster geograficzny 6 urządzeń Brocade VDX 6740 pracujące w oparciu o protokół Trill. Brocade VDX 7640 są swatchami TOR dla 3 lokalizacji, W każdej lokalizacji geograficznej znajdują się 2 switche VDX 7640.
b) Logicznie z funkcjonalnością:
   - NAT/PAT - (Około 130 reguł)
   - regły bezpieczeństwa (około 240 reguł)
   - VPN z integracja do Active Directory MS - około 300 kont
   - X-Forwarded-For HTTP Header dla squid
   - Tunele IpSec
   - polityki PBR
   - polityki filtrowania ruchu na podstawie URL filtering
   - polityki kontroli antywirusowej
   - blokowanie ściągania załączników z określonymi typami dokumentów oraz dokumentów spakowanych na hasło.
   - DoS Protections

1. 1. Przedmiotem zamówienia jest dostawa i instalacja klastra wysokiej dostępności urządzeń Palo Alto Networks zgodnie z poniższą tabelą:

P/N	nazwa	ilość
PAN-PA-1410	Palo Alto Networks PA-1410	2
PAN-PA-1410-ATP-3YR-HA2	PA-1410, Advanced Threat, for one (1) device in an HA pair, 3 years (36 months) term.	2
PAN-PA-1410-GP-3YR-HA2	PA-1410, GlobalProtect subscription, for one (1) device in an HA pair, 3 years (36 months) term.	2
PAN-PA-1410-ADVURL-3YR-HA2	PA-1410, Advanced URL Filtering subscription, for one (1) device in an HA pair, 3 years (36 months) term.	2
PAN-SVC-BKLN-1410-3YR	PA-1410, Partner enabled premium support, 3 years (36 months) term.	2

1. 2. Dostarczone urządzenia muszą być fabrycznie nowe, nieużywane, wyprodukowane nie wcześniej niż 6 miesięcy przed datą zawarcia Umowy.
    - Wszystkie urządzenia i komponenty dostarczone w ramach realizacji niniejszego zamówienia muszą być objęte gwarancją i rozszerzonym wsparciem producenta przez okres 36 miesięcy, liczony od daty odbioru końcowego przedmiotu umowy. Warunki gwarancji i wsparcia producenta zostały określone w punkcie III.
    - Wykonawca zapewni instalację, konfigurację oraz podłączenie do infrastruktury Zamawiającego dostarczonych urządzeń w lokalizacji wskazanej przez Zamawiającego zgodnie z wymaganiami opisanymi poniżej w pkt II.
    - Wykonawca w ramach zamówienia zapewni autoryzowane szkolenie „FIREWALL: KONFIGURACJA I ZARZĄDZANIE (PAN-EDU-210)" dla 4 pracowników Zamawiającego. Szkolenie musi mieć miejsce w autoryzowanym ośrodku szkoleniowym producenta.

II. Wymagania dotyczące instalacji i konfiguracji dostarczonych urządzeń

Rozbudowa wydajności systemów bezpieczeństwa Next Generation Firewall polega w szczególności na:

1. Przeniesienie części usług z klastra urządzeń PA-3220 na nowe urządzenia PA-1410, w tym:
2. Uruchomienie klastra HA na nowych urządzeniach.
3. Fizyczne uruchomienie połączeń (po stronie wykonawcy jest konfiguracja, dostarczenie kabli DAC i patchordów, konfiguracja urządzeń cisco, brocade ICX, oraz clustra Brocade VDX 6740)
    - sieć WAN (uruchomiony protokół BGP) 2x 10G - dwa nie zależne łącza
    - Sieć DMZ - 2x10G LACP do urządzeń cisco i brocade ICX (około 20 sieci DMZ)
    - Sieć LAN - 2x10G LACP - cluster geograficzny 6 urządzeń Brocade VDX 6740
4. Uruchomienie VPN z integracja do Active Directory
5. DoS Protections

Uruchomienie urządzeń ma zapewnić działania obu clustrów (starego klastra i nowego klastra Paloalto) równoległe działanie obu klastrów z podpięciem do istniejącej sieci Zamawiającego oraz umożliwiać płynne przenoszenie usług z klastra urządzeń PAN-PA-3220 na cluster PAN-PA-1410.

Tak przygotowany system ma zapewniać możliwość przenoszenia reguł security i NAT po miedzy klastrami Paloalto, przeniesiona reguła lub grupa reguł security/nat po przeniesieniu ma odrazu działać na nowym klastrze. Procedura ma zapewniać również w razie nie powodzenia powrót do poprzedniej konfiguracji.

Wszelkie rzeczy potrzebne do uruchomienia nowego klustra w tym okablowanie, patchcordy i konfiguracja sieci LAN/WAN/DMZ Zamawiajacego (urządzenia cisco, brocade ICX, cluster brocade VDX 6740) jest po stronie Wykonawcy.

III. Warunki gwarancji i wsparcia producenta dla urządzeń firewall

1. Gwarancja na urządzenia firewall będzie udzielona na okres minimum 36 miesięcy.
    1.1. W trakcie trwania gwarancji Zamawiający będzie uprawniony do pobierania nowych wersji oprogramowania układowego (firmware).
    1.2. Gwarancja będzie realizowana w miejscu instalacji sprzętu przez serwis producenta lub firmę posiadającą autoryzację producenta na świadczenie usług serwisowych, z czasem reakcji do następnego dnia roboczego po dniu przyjęcia zgłoszenia oraz skutecznym czasem naprawy nie dłuższym niż 1 dzień roboczy od dnia reakcji serwisu.
    1.3. Wszystkie urządzenia zostaną dostarczone wraz z pakietami serwisowymi producenta ważnymi przez okres zgodny z okresem gwarancji, obejmującymi minimum:
2. Udzielanie odpowiedzi na pytania dotyczące instalacji, używania i konfiguracji dostarczonych urządzeń i oprogramowania.

3. Bezpośrednie konsultacje telefoniczne oraz poprzez pocztę elektroniczną z inżynierem producenta oraz jego autoryzowanego polskiego przedstawiciela dotyczące bieżących problemów związanych ze sprzętem i oprogramowaniem.
4. Analizę informacji diagnostycznych mającą na celu określenie przyczyny problemu, np. pomoc w interpretacji dokumentacji problemów związanych z instalacją lub kodem.
5. W przypadku znanych defektów oprogramowania przekazywanie informacji o sposobie ich usunięcia lub obejścia, a także udzielanie pomocy w uzyskaniu poprawek, do otrzymania których Zamawiający jest uprawniony w ramach posiadanej licencji.
6. Nieprzerwany i nieograniczony dostęp do zasobów elektronicznych, baz samopomocy, FAQ, baz wiedzy producenta urządzeń.
7. Możliwość telefonicznego oraz elektronicznego zgłaszania awarii dotyczących dostarczonego sprzętu w dni robocze, w godzinach 8:00-16:00.
8. Możliwość sprawdzenia statusu gwarancji i wsparcia poprzez stronę producenta, podając unikatowy numer urządzenia, pobieranie uaktualnień mikrokodu oraz sterowników.
9. W przypadku awarii dysku twardego lub innego nośnika danych powodującej konieczność jego wymiany, uszkodzony nośnik pozostanie u Zamawiającego. Zamawiający nie ponosi żadnych kosztów wymiany nośników danych spowodowanych wystąpieniem awarii.
10. Przy rozwiązywaniu problemów Zamawiający zastrzega sobie prawo do bezpośredniego kontaktu z producentem sprzętu we wszystkich kwestiach dotyczących sprzętu i oprogramowania stanowiącego przedmiot zamówienia, a Wykonawca zobowiązany jest zapewnić możliwość takiego kontaktu.

IV. Warunki równoważności dla urządzeń Palo Alto Networks PA-1410

Zamawiający, biorąc pod uwagę zasady racjonalnego gospodarowania środkami publicznymi, w ramach ochrony inwestycji poczynionej, wymaga aby rozwiązanie równoważne spełniało istniejące parametry systemu posiadanego przez Zamawiającego.

Rozwiązanie równoważne musi zagwarantować utrzymanie obecnej funkcjonalności realizowanej przez klaster wysokiej dostępności firewalli Palo Alto Networks PA-3220, oraz planowanej funkcjonalności realizowanej przez nowy klaster wysokiej dostępności firewalli Palo Alto Networks PA-1410.

Wykonawca zamierzający zaproponować rozwiązanie równoważne zobowiązany jest do dostarczenia 2 klastrów urządzeń Next Generation Firewall o minimalnych parametrach opisanych poniżej w punktach 1 i 2.

Ponadto Wykonawca w takim przypadku będzie zobowiązany do przeniesienia usług sieciowych Zamawiającego z urządzeń Palo Alto Networks na oferowane przez siebie w zakresie, który obejmuje następujące odtworzenie funkcjonalności:

1. Fizycznie połączone są w pare HA, zestawione łączą do:

    1.1. sieć WAN (uruchomiony protokół BGP) 2x 10G - dwa nie zależne łącza
    1.2. sieć DMZ - 2x10G LACP do urządzeń Cisco i Brocade ICX (około 20 sieci DMZ)
    1.3. sieć LAN - 2x10G LACP (uruchomiony protokół ospfv2) - cluster geograficzny 6 urządzeń Brocade VDX 6740 pracujące w oparciu o protokół Trill. Brocade VDX 7640 są switchami TOR dla 3 lokalizacji, W każdej lokalizacji geograficznej znajdują się 2 switche VDX 7640.
2. Odtworzenie działania urządzenia z funkcjonalnością i przeniesienie wszystkich reguł:

    2.1. NAT/PAT - (Około 130 reguł)
    2.2. reguły bezpieczeństwa (około 240 reguł)
    2.3. VPN z integracja do Active Directory MS - około 300 kont
    2.4. X-Forwarded-For HTTP Header dla Squid
    2.5. Tunele IpSec
    2.6. polityki PBR

2.7. polityki filtrowania ruchu na podstawie URL filtering
2.8. polityki kontroli antywirusowej
2.9. blokowanie ściągania załączników z określonymi typami dokumentów oraz dokumentów spakowanych na hasło.
2.10 DoS Protections

Dodatkowo, w przypadku dostarczenia rozwiązania równoważnego Wykonawca zapewni przeszkolenie 6 administratorów Zamawiającego w zakresie instalacji, konfiguracji i administracji urządzeń równoważnych. Szkolenie musi być autoryzowanym/certyfikowanym szkoleniem producenta rozwiązania równoważnego, kończącym się egzaminem skutkującym wydaniem imiennego certyfikatu dla każdego z 6 administratorów Zamawiającego, którzy z wynikiem pozytywnym ukończyli szkolenie oraz zdali egzamin.

1. *Urządzenia równoważne do klastra PA-3220*

1. Wymagania podstawowe

1.1. Muszą to być specjalizowane urządzenia sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako para wysokiej dostępności (HA) w trybach Active/Standby, Active/Active.
1.2. Całość sprzętu i oprogramowania musi być dostarczona i zapewniać wsparcie serwisowe przez jednego tego samego producenta.
1.3. Urządzenia muszą umożliwiać działanie w następujących trybach pracy:
- routera (tzn. w warstwie 3 modelu ISO OSI),
- mostu (tzn. w warstwie 2 modelu ISO OSI),
- w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; musi pracować w trybie przezroczystego łączenia interfejsów w pary),
- w trybie pasywnego nasłuchu (tzw. sniffer/tap).

System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
1.4. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.
1.5. Urządzenia firewall muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu (tzw. data plane) od zasobów służących do zarządzania urządzeniem (tzw. management plane). Akceptowana jest separacja logiczna zasobów zrealizowana za pomocą przypisania dedykowanej ilości rdzeni zasobów procesorów (tzw. CPU core's) do obu z funkcji lub alternatywnie za pomocą oddzielnych dedykowanych procesorów (tzw. CPU) dla każdej z funkcji.
1.6. 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.
1.7. Urządzenia firewall muszą wspierać protokół LACP.
1.8. 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).
1.9. 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.
1.10. Polityka zabezpieczeń firewall musi uwzględniać:
- adresy IP źródłowe i docelowe,
- protokoły i usługi sieciowe,
- aplikacje,
- kategorie URL,
- użytkowników aplikacji i grupy,
- reakcje zabezpieczeń,
- logowanie zdarzeń (początek i koniec sesji)
- strefa wejściowa i wyjściowa

1.11. Urządzenia firewall muszą automatycznie identyfikować aplikacje bez względu na numery portów (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Urządzenie musi wykrywać co najmniej 3500 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz z aplikacjami przemysłowymi (tzw. ICS/OT) np. DNP3, Modbus.
Urządzenia muszą pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI

urządzenia (bez użycia zewnętrznych narzędzi).

1.12. Urządzenia firewall muszą pozwalać na blokowanie transmisji plików wybranego typu, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .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.

1.10. Urządzenia firewall muszą być zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji lub pobierania dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.

1.11. 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 przewidzieć odpowiednie licencje dla minimum 30 administratorów na wszystkie oferowane urządzenia.

1.12. 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.

1.13. Urządzenia firewall muszą umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż: baza lokalna, serwer Radius, serwer TACACS+, serwer AD/LDAP. Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH.

1.14. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
- Microsoft Active Directory,
- Microsoft Exchange
- Terminal Services
- Syslog
- Cisco ISE

1.15. 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.

1.16. 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, połączeniach VPN.

1.17. Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich 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. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.

1.18. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
- reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
- API

1.19. Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESXi i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można następnie wykorzystywać w polityce bezpieczeństwa urządzeń.

1.20. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.

1.21. 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.

1.22. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

1.23. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami informacji o NAT.

1.24. Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju. Konieczna jest obsługa Syslog za pomocą transportu UDP, TCP, SSL oraz obsługa formatów IETF oraz BSD.

1.25. Urządzenia firewall muszą obsługiwać możliwość deszyfracji ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.

1.26. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub

wykluczyć z operacji deszyfrowania i inspekcji - rozdzielny od polityk bezpieczeństwa.

1.27. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS który nie ma zostać odszyfrowany, ale poddany sprawdzeniu czy certyfikat serwera nie wygasł oraz sprawdzeniu czy certyfikat nie pochodzi od zaufanego wystawcy. W takim przypadku urządzenie musi umożliwiać blokadę takiej sesji użytkownika.

1.28. Wykonywanie operacji deszyfracji 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.

1.29. Wykonywanie operacji deszyfracji ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL (w przypadku, gdy jest wymagane jego dostarczenie) albo możliwość wykorzystania własnej utworzonej na urządzeniu listy URL które mają podlegać deszyfracji albo być z niej wykluczone (tzw. wyjątek).

1.30. Urządzenie firewall musi posiadać 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.

1.31. 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, TLS_CHACHA20_POLY1305_SHA256.

1.32. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości sesji w odniesieniu do źródłowego lub docelowego adresu IP.

1.33. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) dla aplikacji i użytkowników.

1.34. 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).

1.35. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.

1.36. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.

1.37. Urządzenia firewall muszą zapewniać inspekcję komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu blokowania tuneli SSH.

1.38. Urządzenia firewall muszą obsługiwać funkcję DNS proxy.

1.39. Urządzenia firewall muszą obsługiwać funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta musi być realizowana na bazie technologii SSL VPN oraz IPSec. Jeżeli oprogramowania klienta Remote Access VPN dla laptopów z systemem klienckim Windows wymaga licencji – należy dostarczyć licencję na maksymalną wydajność oraz maksymalną ilość dla oferowanego typu urządzeń.

1.40. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.

1.41. Urządzenia firewall dla zdalnego dostępu VPN muszą umożliwiać następujące funkcjonalności:

- Realizacja VPN dla aplikacji HTML/HTML5 w trybie przeglądarkowym (tzw. Clientless VPN)
- Zestawianie zdalnego dostępu dla urządzeń mobilnych tzw. smart devices. Telefony/tablety bazujące na systemach operacyjnych: Apple iOS i Google Android.
- Dostępność oprogramowania klienckiego VPN dla urządzeń mobilnych z systemami: Apple iOS (10-16), Android (6-13), Win UWP
- Dostępność oprogramowania klienta VPN dla stacji/laptopów dla następujących systemów operacyjnych: Windows 8-11; Windows 10 UWP; iOS 10-14; MacOS 10.15-13; Google Android 6-11; Linux CentOS, RHEL, Ubuntu;
- Sprawdzanie informacji o systemie operacyjnym, aktualizacji poprawek OS, aktualizacji oprogramowania antywirusowego itp. dla systemów Windows.
- Sprawdzanie obecności konta urządzenia w systemie katalogowym Windows AD dla systemów Windows.
- Możliwość pomijania tunelu zdalnego dostępu VPN dla specyficznych aplikacji, domeny DNS, aplikacji video. Dla podłączających się stacji/laptopów Windows i MacOS.
- Dodatkowa identyfikacja urządzeń użytkownika na bazie unikalnego identyfikatora innego niż adres IP (Windows – MachineGuid, Android – Android ID, iOS – UDID) pozwalająca na blokadę dostępu VPN dla wybranego urządzenia. Np. blokada dostępu VPN dla urządzenia zainfekowanego.
- Możliwość automatycznego (bez ingerencji administratora) zablokowania dostępu poprzez RA VPN urządzenia skompromitowanego do chronionych zasobów.

1.42. Producent oferowanego rozwiązania musi być obecny w najnowszym rynkowym raporcie Gartner Magic Quadrant for Enterprise Network Firewalls w części (tzw. ćwiartce) Leaders.

1.43. Dostarczane razem z urządzeniami subskrypcje, licencje, gwarancje muszą funkcjonować 36 miesięcy.

1.44. W przypadku potrzeby wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby dyski zostały wymontowane z urządzenia i pozostały w jego siedzibie w celu bezpiecznej utylizacji.

2. Wymagania dodatkowe

Należy dostarczyć 2 szt. urządzeń, które będą pracowały jako 1 para w układzie HA.
Razem z urządzeniami muszą zostać dostarczone następujące typy i ilości modułów połączeniowych. Ilość dla zestawu 2 urządzeń głównych:

1. Do HA: **4** szt. SFP+ 10GE wariant SR
2. Do LAN**: 4** szt. SFP+ 10GE wariant SR

Każde z urządzeń musi (poza wymaganiami wspólnymi), spełniać dodatkowo wymagania:

1. Urządzenie musi być wyposażone w minimum:
   1.1. dedykowany port Ethernet do zarządzania urządzeniem o prędkościach 10/100/1000Mbps
   1.2. dedykowany port konsoli do zarządzania urządzeniem w standardzie RJ45 bądź Micro USB,
   1.3. 12 wbudowanych interfejsów Ethernet (RJ45) pracujących z prędkościami 10/100/1000Mbps.
   1.4. 4 wbudowane gniazda pozwalające na obsadzenie modułami 1Gbps SFP.
   1.5. 4 wbudowane elastyczne gniazda pozwalających na obsadzenie modułami 1Gbps SFP oraz 10Gbps SFP+. Jeżeli urządzenie nie wspiera gniazd elastycznych, musi posiadać 4 gniazda 1Gbps SFP oraz 4 gniazda 10Gbps SFP+.
   1.6. 1 wbudowany dedykowany interfejs HA w formie gniazda 10Gbps SFP+.
   1.7. Musi być wyposażone w zasób dyskowy (niemechaniczny) o wielkości co najmniej 220 GB na potrzeby systemu operacyjnego. W przypadku procedury wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby zasoby dyskowe zostały wymontowane z urządzenia i pozostały w jego siedzibie w celu bezpiecznej utylizacji.
   1.8. Musi być wyposażone w co najmniej 2 zasilacze typu AC 230V pracujące redundantnie. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.
   1.9. Urządzenie musi być przeznaczone do montażu w szafie Rack 19”.
2. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
   2.1. 4,1 Gbps dla rozpoznawania i kontroli aplikacji.
   2.2. 2,1 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: włączone wszystkie sygnatury IPS, antywirus, antyspyware, blokowanie typów plików, z włączonym logowaniem na dyski urządzenia.
   2.3. 2,3 Gbps dla IPSec VPN,
   2.4. 45000 nowych sesji na sekundę.
   2.5. 950000 równoległych sesji
3. Musi obsługiwać nie mniej niż 10 wirtualnych routerów, posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu, w pojedynczej wirtualnej instancji firewall. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia.
4. Urządzenie musi posiadać co najmniej 180 stref bezpieczeństwa.
5. Urządzenie musi posiadać możliwość licencyjnego ustanowienia co najmniej 6 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.
6. Urządzenie musi posiadać architekturę z odseparowanymi zasobami. Procesory zarządzające oraz pamięć (tzw. Management Plane) muszą być oddzielne od procesorów i pamięci przetwarzających ruch sieciowy (tzw. Data Plane).
7. Nadmierne obciążenie ruchem sieciowym (Data Plane) urządzenia nie może blokować funkcjonowania części zarządzającej (Management Plane). Nie może powodować problemów z konfigurowaniem czy monitorowaniem urządzenia, dostępem do interfejsu GUI i CLI.
8. Musi umożliwiać zdefiniowanie nie mniej niż 9900 reguł polityki bezpieczeństwa oraz 2900 reguł NAT.
9. Urządzenie musi posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
10. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur oraz powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.
11. Urządzenie musi posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.
12. Urządzenie musi 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 48h) i pochodzić od tego samego producenta co firewall.

13. Urządzenie musi posiadać funkcję anty-spyware. Baza sygnatur musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.
14. Urządzenie musi posiadać funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (Machine Learning - ML) aktualizowanych dynamicznie przez producenta.
15. Wykrywanie za pomocą algorytmów musi odbywać się lokalnie na urządzeniu jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antywirus oraz funkcji filtrowania URL.
16. Wymagane jest posiadanie funkcji wykrywania za pomocą ML (Machine Learning) dla następujących danych: złośliwych plików wykonywalnych (tzw. PE), złośliwych skryptów PowerShell, złośliwych stron / ataków Phishing, złośliwych skryptów JavaScript.
17. Dodatkowo rozwiązanie musi posiadać możliwość analizy, identyfikacji oraz blokowania wcześniej nieznanej komunikacji C2 (command-and-control) oraz spyware w oparciu o nauczanie maszynowe realizowane w chmurze producenta, przy czym:
18. Wymagana analiza i detekcja musi umożliwiać blokowanie wykrytej komunikacji C2 w czasie rzeczywistym,
19. Analiza i wykrywanie nieopisanych wcześniej w sygnaturach połączeń C2 muszą być możliwe minimum dla ruchu typu: http, http2, ssl oraz niezidentyfikowanych przez firewall aplikacji w oparciu o TCP i UDP,
20. Urządzenie musi posiadać funkcję filtrowania URL.
21. Urządzenie musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (a nie tylko filtrującego) ruch w politykach bezpieczeństwa.
22. 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.
23. Wymagane jest posiadanie oddzielnych kategorii URL dla zagrożeń typu malware, phishing, C2C oraz dla ostatnio zarejestrowanych domen.
24. Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania kategorii URL.
25. Funkcjonalność musi zapewniać możliwość blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (Machine Learning, ML) aktualizowanych dynamicznie przez producenta. Wykrywanie za pomocą algorytmów ML musi odbywać się lokalnie na urządzeniu jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antivirus oraz funkcji filtrowania URL.

3. Urządzenia równoważne do klastra PA-1410

3.1. Wymagania podstawowe

3.1.1. Muszą to być specjalizowane urządzenia sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako para wysokiej dostępności (HA) w trybach Active/Standby, Active/Active.

3.1.2. Całość sprzętu i oprogramowania musi być dostarczona i zapewniać wsparcie serwisowe przez jednego tego samego producenta.

3.1.3. Urządzenia muszą umożliwiać działanie w następujących trybach pracy:
- routera (tzn. w warstwie 3 modelu ISO OSI),
- mostu (tzn. w warstwie 2 modelu ISO OSI),
- w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; Musi pracować w trybie przezroczystego łączenia interfejsów w pary.).
- w trybie pasywnego nasłuchu (tzw. sniffer/tap).

System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.

3.1.4. Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45, w co najmniej jeden dedykowany port zarządzający realizowany jako port Ethernet 10/100/1000 lub jako port SFP z wkładką 1000BASE-T.

3.1.5. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.

3.1.6. Urządzenia firewall muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu (tzw. data plane) od zasobów służących do zarządzania urządzeniem (tzw. management plane). Akceptowana jest separacja logiczna zasobów zrealizowana za pomocą przypisania dedykowanej ilości rdzeni zasobów procesorów (tzw. CPU cores) do obu z funkcji lub alternatywnie za pomocą oddzielnych dedykowanych procesorów (tzw. CPU) dla każdej z funkcji.

3.1.7. 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.

3.1.8. Urządzenia firewall muszą wspierać protokół LACP.

3.1.9. 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).

3.1.10. 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.

3.1.11. Polityka zabezpieczeń firewall musi uwzględniać:
- adresy IP źródłowe i docelowe,
- protokoły i usługi sieciowe,
- aplikacje,
- kategorie URL,
- użytkowników aplikacji i grupy,
- reakcje zabezpieczeń,
- logowanie zdarzeń (początek i koniec sesji)
- strefa wejściowa i wyjściowa

3.1.12. Urządzenia firewall muszą automatycznie identyfikować aplikacje bez względu na numery portów (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Urządzenie musi wykrywać co najmniej 3500 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz z aplikacjami przemysłowymi (tzw. ICS/OT) np. DNP3, Modbus.
Urządzenia muszą pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia (bez użycia zewnętrznych narzędzi).

3.1.13. Urządzenia firewall muszą pozwalać na blokowanie transmisji plików wybranego typu, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .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.

3.1.14. Urządzenia firewall muszą być zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji lub pobierania dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.

3.1.15. 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 przewidzieć odpowiednie licencje dla minimum 30 administratorów na wszystkie oferowane urządzenia.

3.1.16. 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.

3.1.17. Urządzenia firewall muszą umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż: baza lokalna, serwer Radius, serwer TACACS+, serwer AD/LDAP. Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH.

3.1.18. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
- Microsoft Active Directory,
- Microsoft Exchange
- Terminal Services
- Syslog
- Cisco ISE

3.1.19. 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.

3.1.20. 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, połączeniach VPN.

3.1.21. Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich 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. Na urządzeniu musi być również dostępne tworzenie raportów o

aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.

3.1.22. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
- reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
- API

3.1.23. Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESXi i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można następnie wykorzystywać w polityce bezpieczeństwa urządzeń.

3.1.24. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.

3.1.25. 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.

3.1.26. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

3.1.27. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami informacji o NAT.

3.1.28. Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju. Konieczna jest obsługa Syslog za pomocą transportu UDP, TCP, SSL oraz obsługa formatów IETF oraz BSD.

3.1.29. Urządzenia firewall muszą obsługiwać możliwość deszyfracji ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.

3.1.30 Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji - rozdzielny od polityk bezpieczeństwa.

3.1.31. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS który nie ma zostać odszyfrowany, ale poddany sprawdzeniu czy certyfikat serwera nie wygasł oraz sprawdzeniu czy certyfikat nie pochodzi od zaufanego wystawcy. W takim przypadku urządzenie musi umożliwiać blokadę takiej sesji użytkownika.

3.1.32. Wykonywanie operacji deszyfracji 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.

3.1.33. Wykonywanie operacji deszyfracji ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL (w przypadku, gdy jest wymagane jego dostarczenie) albo możliwość wykorzystania własnej utworzonej na urządzeniu listy URL które mają podlegać deszyfracji albo być z niej wykluczone (tzw. wyjątek).

3.1.34. Urządzenie firewall musi 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.

3.1.35. 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, TLS_CHACHA20_POLY1305_SHA256.

3.1.36. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości sesji w odniesieniu do źródłowego lub docelowego adresu IP.

3.1.37. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) dla aplikacji i użytkowników.

3.1.38. 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).

3.1.39. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.

3.1.40. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.

3.1.41. Urządzenia firewall muszą zapewniać inspekcję komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu blokowania tuneli SSH.

3.1.42. Urządzenia firewall muszą obsługiwać funkcję DNS proxy.

3.1.43. Urządzenia firewall muszą obsługiwać funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta musi być realizowana na bazie technologii SSL VPN oraz IPSec. Jeżeli oprogramowania klienta Remote Access VPN dla laptopów z systemem klienckim Windows wymaga licencji – należy dostarczyć licencję na maksymalną wydajność oraz maksymalną

ilość dla oferowanego typu urządzeń.

3.1.44. Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.

3.1.45. Urządzenia firewall dla zdalnego dostępu VPN muszą umożliwiać następujące funkcjonalności:
- Realizacja VPN dla aplikacji HTML/HTML5 w trybie przeglądarkowym (tzw. Clientless VPN)
- Zestawianie zdalnego dostępu dla urządzeń mobilnych tzw. smart devices. Telefony/tablety bazujące na systemach operacyjnych: Apple iOS i Google Android.
- Dostępność oprogramowania klienckiego VPN dla urządzeń mobilnych z systemami: Apple iOS (10-16), Android (6-13), Win UWP
- Dostępność oprogramowania klienta VPN dla stacji/laptopów dla następujących systemów operacyjnych: Windows 8-11; Windows 10 UWP; iOS 10-14; MacOS 10.15-13; Google Android 6-11; Linux CentOS, RHEL, Ubuntu;
- Sprawdzanie informacji o systemie operacyjnym, aktualizacji poprawek OS, aktualizacji oprogramowania antywirusowego itp. dla systemów Windows.
- Sprawdzanie obecności konta urządzenia w systemie katalogowym Windows AD dla systemów Windows.
- Możliwość pomijania tunelu zdalnego dostępu VPN dla specyficznych aplikacji, domeny DNS, aplikacji video. Dla podłączających się stacji/laptopów Windows i MacOS.
- Dodatkowa identyfikacja urządzeń użytkownika na bazie unikalnego identyfikatora innego niż adres IP (Windows – MachineGuid, Android – Android ID, iOS – UDID) pozwalająca na blokadę dostępu VPN dla wybranego urządzenia. Np. blokada dostępu VPN dla urządzenia zainfekowanego.
- Możliwość automatycznego (bez ingerencji administratora) zablokowania dostępu poprzez RA VPN urządzenia skompromitowanego do chronionych zasobów.

4.1.46. Producent oferowanego rozwiązania musi być obecny w najnowszym rynkowym raporcie Gartner Magic Quadrant for Enterprise Network Firewalls w części (tzw. ćwiartce) Leaders.

4.1.47. Dostarczane razem z urządzeniami subskrypcje, licencje, gwarancje muszą funkcjonować 36 miesięcy.

4.1.48. W przypadku potrzeby wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby dyski zostały wymontowane z urządzenia i pozostały w jego siedzibie w celu bezpiecznej utylizacji.

3.2. Wymagania dodatkowe

Należy dostarczyć 2 szt. urządzeń, które będą pracowały jako 1 para w układzie HA.
Razem z urządzeniami muszą zostać dostarczone następujące typy i ilości modułów połączeniowych. Ilość dla zestawu 2 urządzeń głównych:

1. Do HA: **4** szt. SFP+ 10GE wariant SR
2. Do LAN**: 4** szt. SFP+ 10GE wariant SR

Każde z urządzeń musi (poza wymaganiami wspólnymi), spełniać dodatkowo wymagania:

3.2.1. Urządzenie musi być wyposażone w minimum:

3.2.2. minimum 8 portów Ethernet RJ45 wspierających prędkości 10/100/1000Mbps;

3.2.3. minimum 4 porty Ethernet RJ45 wspierających 5G/2.5G/1GE/100Mbps z zasilaniem PoE z budżetem 150W mocy oraz możliwością udostępnienia na porcie 50W mocy;

3.2.4. minimum 6 portów Ethernet SFP (akceptujących moduły 1GE SFP)

3.2.5. minimum 4 porty Ethernet SFP+ (akceptujących moduły 10GE SFP+ oraz 1GE SFP)

3.2.6. minimum 1 port dla celów połączenia urządzeń w HA: minimum 1x 10GE SFP+ (lub szybszy) oraz minimum 2x 1GE (SFP lub RJ45) (lub szybszy). Porty te muszą być traktowane jako dodatkowe względem wymaganych powyżej. Nie dopuszcza się liczenia jako HA, portów wymaganych wcześniej.

3.2.7. Musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 100 GB na potrzeby systemu operacyjnego i logów.

3.2.8. W przypadku procedury wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby zasób dyskowy zostały wymontowany z urządzenia i pozostał w jego siedzibie w celu bezpiecznej utylizacji.

3.2.9. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
- Minimum 6,8 Gbps dla rozpoznawania i kontroli aplikacji,
- Minimum 3,2 Gbps dla rozpoznawania kontroli aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Antywirus, Antyspyware, blokowanie typów plików, z włączonym logowaniem na dysk urządzenia.
- Minimum 4,6 Gbps wydajności IPSec VPN.
- Minimum 100 000 nowych sesji na sekundę.
- Minimum 945 000 równoległych sesji
- Minimum 1500 tuneli klienckich VPN
- Minimum 2500 sąsiedztw IKE (IPSec)

3.2.10. Musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i

umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia.

3.2.11. Musi umożliwiać zdefiniowanie nie mniej niż 1500 reguł polityki bezpieczeństwa oraz 3000 reguł NAT.

3.2.12. Każde z urządzeń musi być wyposażone w dwa zasilacze typu AC 230V pracujące redundantnie. Zasilacze muszą być wymienne z możliwością podmiany uszkodzonego zasilacza w trakcie pracy urządzenia.

3.2.13. Urządzenie musi być przeznaczone do montażu w szafie Rack 19".

3.2.14. Urządzenie musi posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

3.2.15. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur oraz powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.

3.2.16. Urządzenie musi posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.

3.2.17. Urządzenie musi 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 48h) i pochodzić od tego samego producenta co firewall.

3.2.18. Urządzenie musi posiadać funkcję anty-spyware. Baza sygnatur musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.

3.2.19. Urządzenie musi posiadać funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (Machine Learning - ML) aktualizowanych dynamicznie przez producenta.

3.2.20. Wykrywanie za pomocą algorytmów musi odbywać się lokalnie na urządzeniu jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antywirus oraz funkcji filtrowania URL.

3.2.21. Wymagane jest posiadanie funkcji wykrywania za pomocą ML (Machine Learning) dla następujących danych: złośliwych plików wykonywalnych (tzw. PE), złośliwych skryptów PowerShell, złośliwych stron / ataków Phishing, złośliwych skryptów JavaScript.

3.2.22. Dodatkowo rozwiązanie musi posiadać możliwość analizy, identyfikacji oraz blokowania wcześniej nieznanej komunikacji C2 (command-and-control) oraz spyware w oparciu o nauczanie maszynowe realizowane w chmurze producenta, przy czym:
- wymagana analiza i detekcja musi umożliwiać blokowanie wykrytej komunikacji C2 w czasie rzeczywistym,
- analiza i wykrywanie nieopisanych wcześniej w sygnaturach połączeń C2 muszą być możliwe minimum dla ruchu typu: http, http2, ssl oraz niezidentyfikowanych przez firewall aplikacji w oparciu o TCP i UDP.
- Urządzenie musi posiadać funkcję filtrowania URL.
- Urządzenie musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (a nie tylko filtrującego) ruch w politykach bezpieczeństwa.
- 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.
- Wymagane jest posiadanie oddzielnych kategorii URL dla zagrożeń typu malware, phishing, C2C oraz dla ostatnio zarejestrowanych domen.
- Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania kategorii URL.

3.2.23. Funkcjonalność musi zapewniać możliwość blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (Machine Learning, ML) aktualizowanych dynamicznie przez producenta. Wykrywanie za pomocą algorytmów ML musi odbywać się lokalnie na urządzeniu jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antivirus oraz funkcji filtrowania URL.