Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

CEL POSTĘPOWANIA:

Celem postępowania jest zakup klastra sprzętowego wysokiej dostępności (HA) dwóch urządzeń sieciowych o funkcjonalności load balancera polegającej na równoważeniu obciążeń i rozdzielaniu ruchu pomiędzy aplikacje/serwery w celu optymalizacji wydajności, efektywności i przepustowości infrastruktury wraz z oprogramowaniem o minimalnej funkcjonalności opisanej poniżej.

System musi realizować co najmniej następujące funkcje (posiadać moduły funkcjonalne):

- Moduł Load Balancera umożliwiający rozkład ruchu pomiędzy serwerami.
- Moduł Firewalla stanowego.
- Moduł ochrony DNS oraz globalnego równoważenia obciążenia za pomocą protokołu DNS.
- Moduł uwierzytelnienia do aplikacji oraz SSL VPN.
- Moduł Web Application Firewalla.
- Posiadać subskrypcję dla serwisu reputacyjnego.
- Posiadać subskrypcję dla serwisu z sygnaturami aktualnych kampanii zagrożeń w Internecie.

SZCZEGÓŁOWE WYMAGANIA DLA DOSTARCZANYCH URZĄDZEŃ:

I. Opis wymagań:

1. Wszystkie wymienione w niniejszym dokumencie i opisane szczegółowo funkcje, muszą być dostępne w obrębie jednego urządzenia fizycznego.
2. Wszystkie wymienione w niniejszym dokumencie funkcje (poza subskrypcjami dla serwisu reputacyjnego, serwisu z sygnaturami aktualnych kampanii zagrożeń w Internecie) muszą być licencjami, które nie mają ograniczeń czasowych i nie wymagają przedłużenia (są licencjami wieczystymi).
3. Zamawiający nie dopuszcza rozwiązania realizowanego w postaci maszyny (maszyn) wirtualnej w środowisku serwerowym (Vmware, Hyper-V, vcloud, KVM, Oracle VM, VirtualBox..

II. Szczegółowy opis funkcji urządzenia. Urządzenie musi realizować co najmniej następujące funkcjonalności:

1. System musi umożliwiać realizację rozkład ruchu pomiędzy serwerami:

1.1 System musi umożliwiać realizację rozdziału ruchu w oparciu o informację z warstw 4-7 modelu ISO/OSI.
1.2 System musi realizować obsługę inteligentnego równoważenia ruchu dla farm serwerów przy wsparciu dla protokołów: TCP, UDP, FTP, TFTP, http, SSL/TLS, DNS, RADIUS, SQL, RDP SSH PPTP NTP MQTT MQTT-TLS ISAKMP SMTP SIP.
1.3 System musi mieć możliwość balansowania ruchu w oparciu o algorytmy:
    1.3.1 Round Robin
    1.3.2 cykliczna dla usługi
    1.3.3 cykliczna dla serwera
    1.3.4 ważona dla usługi
    1.3.5 ważona dla serwera
    1.3.6 dynamiczna ważona dla usługi
    1.3.7 dynamiczna ważona dla serwera
    1.3.8 obserwowana
    1.3.9 przewidywana
    1.3.10 obciążenie serwerów
    1.3.11 ilość połączeń
    1.3.12 ważona ilość połączeń dla serwerów
    1.3.13 ważona ilość połączeń dla usługi
    1.3.14 czas odpowiedzi
    1.3.15 ilość sesji
    1.3.16 ważona dla ilości sesji do serwerów
    1.3.17 ważona dla ilości sesji do usługi
    1.3.18 hashing (URL, Domain, source IP, Destination IP)
1.4 System musi umożliwiać mechanizm dowiązania sesji (session persistence) w oparciu o:
    1.4.1 cookie (hash/passive/insert lub rewrite),
    1.4.2 adres źródłowy,
    1.4.3 adres docelowy,
    1.4.4 identyfikator sesji SSL,
    1.4.5 SESSIONID,
    1.4.6 SIP call,
    1.4.7 Hash,
    1.4.8 Host,
    1.4.9 Msrdp,
    1.4.10 Universal (wybranie dowolnego fragmentu payloadu i utworzenie na jego podstawie profilu persystencji.
1.5 System ma umożliwiać monitorowanie stanów serwerów i na tej podstawie dokonywania decyzji o przełączaniu w oparciu o:
    1.5.1 ICMP,
    1.5.2 TCP,
    1.5.3 UDP,
    1.5.4 HTTP,
    1.5.5 HTTP/2,
    1.5.6 HTTPS,
    1.5.7 Inband,
    1.5.8 SNMP DCA,

1.5.9 Server (co najmniej: ServerBandwidth, CPUPercentUsage, MemoryUsage, TotalClientCount),
1.5.10 Skrypty własne.

1.6 System ma wspierać content switching w oparciu o:
1.6.1 polityki: URL, URL query, URL wildcard Domain, Source IP, Destination IP, Nagłówek http, Dane HTTP i TCP, UDP,
1.6.2 protokoły w przychodzących pakietach.

1.7 System musi umożliwiać obsługę list kontroli dostępu dla 3 i 4 warstwy ISO/OSI.

1.8 System musi umożliwiać zabezpieczenia przed atakami DNS, przynajmniej takimi jak DNS query floods, DNS amplification, zabezpieczenie przed atakami SYN flood.

1.9 Selektywną kompresję danych.

1.10 Terminację sesji SSL.

1.11 Rozwiązanie musi pracować w trybie pełnego proxy.

1.12 Praca w trybie pełnego proxy nie może powodować degradacji wydajności rozwiązania.

1.13 Buforowanie połączeń TCP w przypadku osiągnięcia zadanej ilości sesji dla danego serwera.

1.14 Wsparcie dla HTTP/2, w tym wsparcie dla kompresji nagłówków.

1.15 System musi posiadać funkcję definiowania maksymalnej ilości obsługiwanych przez dany serwer połączeń, w przypadku przekroczenia zdefiniowanej wartości musi istnieć możliwość wysłania klientowi strony błędu lub przekierowania klienta na inny serwer.

1.16 System musi zapewniać możliwość klonowania puli serwerów umożliwiając wysyłanie kopii ruchu do zewnętrznych systemów monitoringu lub urządzeń typu IDS/IPS.

1.17 System musi umożliwiać obsługę sieci co najmniej w zakresie: Routingu statycznego, Routingu dynamicznego OSPF, RIP, BGP, IS-IS, Link Aggregation, 802.3ad, VLAN 802.1q Jumbo Frames, z wykorzystaniem integracji z Equal Cost Multi-Path (ECMP).

1.18 System musi wspierać wysoką dostępność: Active/passive Active/active Connection Mirroring.

1.19 Urządzenie powinno implementować TCP proxy z mechanizmem zamykania okna w stronę serwera www w przypadku zbyt wolnego odbierania danych przez zdalnego klienta.

1.20 Urządzenie musi mieć możliwość strojenia profili połączeń TCP, w tym co najmniej:
1.20.1 Ustawienia timeout idle,
1.20.2 keep alive interval,
1.20.3 zero window timeout,
1.20.4 Initial Receive Window Size,
1.20.5 Wyboru algorytmu wykrywania natłoku,
1.20.6 Wsparcia hybrydowych algorytmów wykrywania natłoku, opartych o stratę pakietów i round-trip-time,
1.20.7 Mechanizmu rate pacing,
1.20.8 określenia maksymalnego wielkości bufora per połączenie TCP celem ochrony przed wysyceniem pamięci,
1.20.9 określenia maksymalnego bufora wysyłania i odbioru (send/receive buffer).

1.21 Urządzenie musi mieć możliwość włączenia ignorowania nagłówków przeglądarki dotyczących cachowania (Cache-control).
1.22 Urządzenie musi umożliwiać selektywne cachowanie zwracanego kontentu a cachowanie powinno być zależne od:
  1.22.1 Listy URN-ów i prefixów URN-ów z których zwracany jest kontent,
  1.22.2 Maksymalnej wielkości zwracanego obiektu,
  1.22.3 minimalnej wielkości zwracanego obiektu.
1.23 Powinna istnieć możliwość ograniczania wielkości cachu, ilości cachowanych obiektów celem ochrony pamięci urządzenia przed przepełnieniem.
1.24 Urządzenie musi wspierać multipleksacje wielu zapytań http w tej samej sesji TCP.
1.25 Urządzenie musi umożliwiać kompresję zwracanej zawartości http. Użycie kompresji powinno być zależne od:
  1.25.1 Listy dozwolonych URI,
  1.25.2 Listy wykluczonych URI,
  1.25.3 Listy możliwych do kompresji Content-Type,
  1.25.4 Listy wykluczonych Content-Type,
  1.25.5 Minimalnej wielkości zwracanego obiektu.
1.26 Kierowanie ruchu do odpowiedniej pooli zasobów:
  1.26.1 Urządzenie powinno realizować mechanizm kierowania żądań od użytkowników końcowych do pool (grup) zasobów serwerowych na podstawie następujących atrybutów:
    1.26.1.1 Wartości http hostname, początku/końca nagłówka hostname, ciąg znaków znajdujący się w nagłówku hostname,
    1.26.1.2 port,
    1.26.1.3 metody http,
    1.26.1.4 nazwy cookie, ciągu znaków na początku/końcu nazwy cookie, ciągu znaku zawartego w nazwie cookie,
    1.26.1.5 URN-a, oraz ciągu znaków występujących na początku/końcu lub zawartych w URN-ie,
    1.26.1.6 User agent,
    1.26.1.7 Dowolnego nagłówka lub kombinacji nagłówków,
    1.26.1.8 Wykorzystania cipherów w TLS,
    1.26.1.9 Common Name Klienta, oraz ciągu znaków występujących na początku/końcu lub zawartych w Common Name.
  1.26.2 Reguły kierowania żądań powinny wymuszać co najmniej następujące akcje:
    1.26.2.1 Wybór pooli zasobów (grupy IP adresów i portów),
    1.26.2.2 Kierowania żądania do konkretnego adresu IP,
    1.26.2.3 Redyrekcji,
    1.26.2.4 Wyłączanie / włączanie ochrony aplikacyjnej,
    1.26.2.5 Wybór polityki ochrony aplikacyjnej,
    1.26.2.6 Włączania/ wyłączania cachowania,
    1.26.2.7 Włączania/ wyłączania kompresji,
    1.26.2.8 Dodania / usunięcia nagłówka / cookie http,
    1.26.2.9 Wyboru parametrów profilu (zestawu parametrów, w tym CA, certyfikatu, klucza) dla połączeń w stronę serwerów aplikacyjnych.

1.26.3 Powinna istnieć możliwość nadpisania statycznych reguł kierowania ruchu w języku skryptowym, na podstawie dowolnych atrybutów żądania http, oraz stanu sesji zapisanego w pamięci urządzenia.

1.27 System musi zapewniać obsługę certyfikatów z kluczami typu ECDSA wykorzystującymi krzywe eliptyczne (ECC) zarówno od strony klienta, jak i od strony puli serwerów,

1.28 Sprzętowe wsparcie dla algorytmów AES, AES-GCM, RSA, DSA, DH, ECDSA, ECDH, SHA2. Wsparcie dla Perfect Forward Secrecy.

1.29 Dla protokołu TLS 1.2 wymagana jest obsługa AES-GCM zarówno od strony klienta, jak i od strony puli serwerów.

1.30 Wsparcie dla protokołu TLS 1.3.

1.31 System musi zapewniać obsługę certyfikatów podpisanych funkcją skrótu SHA-2 zarówno od strony klienta, jak i od strony puli serwerów.

1.32 System musi posiadać funkcję walidacji certyfikatów klientów łączących się przy wykorzystaniu protokołu SSL.

1.33 System musi obsługiwać sieci VLAN w standardzie 802.1q.

1.34 System musi obsługiwać agregację linków w standardzie 802.3ad (LACP).

1.35 System musi obsługiwać Jumbo Frames.

1.36 System musi posiadać funkcjonalność bramy VXLAN oraz NVGRE.

1.37 Klucze prywatne zapisane na dysku urządzenia muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej.

1.38 Rozwiązanie musi posiadać wbudowany w system operacyjny język skryptowy, posiadający co najmniej następujące cechy:

1.38.1 Analiza, zmiana oraz zastępowanie parametrów w nagłówku http oraz w zawartości pakietów,

1.38.2 Obsługa (parsowanie, modyfikacja, kreowanie odpowiedzi) protokołów: http, http2, WebSocket, DNS, RADIUS,

1.38.3 Język skryptowy musi umożliwiać dynamiczne przypisanie polityki bezpieczeństwa aplikacyjnego w oparciu o dowolną kombinację atrybutów http, SSL/TLS.Parsowanie parametrów komunikacji TLS/SSL, w szczególności odczyt certyfikatów X.509 i wstrzykiwanie odczytanych parametrów w formie nagłówków http,

1.38.4 Możliwość zdefiniowania reakcji na zagrożenie wykryte przez Web Application Firewall na podstawie danych dostarczonych przez WAF, odczytanych w komunikacji http, SSL, WebSocket oraz historycznych atrybutów konfiguracji (kontekstu).

1.38.5 Język skryptowy musi być oparty o Tool Command Language i mieć możliwość delegowania złożonych zadań do silnika NodeJS oraz użycia bibliotek „społecznościowych”, celem np. parsowania protokołów jeszcze nie zaimplementowanych w rozwiązaniu Application Delivery Controller.

2. System musi umożliwiać realizację firewalla stanowego:

2.1 Konfigurację reguł firewallowych za pomocą wbudowanego w system interfejsu graficznego.

2.2 Rozwiązanie powinno śledzić i ograniczać wystąpienia anomalii warstw niższych, w tym: IPv4, IPv6, TCP, UDP, ICP.

2.3 Rozwiązanie powinno zawierać system sztucznej inteligencji analizujący na bieżąco ruchu i wykrywające ilościowe anomalie ruchu.

2.4 Rozwiązanie powinno zawierać w pełni funkcjonalny firewall warstwy 4.
2.5 Rozwiązanie powinno być wyposażone w system ochrony przed atakami DDoS realizowany przynajmniej częściowo za pomocą dedykowanych komponentów hardware.
2.5.1 Rozwiązanie powinno obsłużyć sprzętowo mitygację minimum 100 wektorów ataków DDoS.
2.6 Rozwiązanie powinno umożliwiać uruchomienie proxy SSH, które umożliwia np. blokowanie ściągania lub wgrywania plików po SCP lub SFTP, ustawienie czy użytkownik ma dostęp do shella.

3. System ochrony DNS musi realizować co najmniej następujące funkcjonalności:
3.1.1 DNS Autorytatywny,
3.1.2 Global Server Load Balancing,
3.1.3 Dynamiczne podpisywanie domen DNS SEC,
3.1.4 DNS Caching,
3.1.5 DNS Resolver,
3.1.6 Walidacja podpisów odpowiedzi DNS SEC,
3.1.7 Rozkład ruchu pomiędzy serwerami DNS innych producentów,
3.1.8 Ochrona przed atakami DDoS na protokół DNS,
3.1.9 Ochrona przed atakami DDoS na niższe (niż DNS) protokoły w modelu ISO/OSI,
3.2 System musi natywnie wspierać IPv4 i IPv6.
3.3 System musi obsługiwać sieci VLAN w standardzie 802.1q.
3.4 System musi obsługiwać agregację linków w standardzie 802.3ad (LACP).
3.5 Rozwiązanie powinno wspierać rozrzucanie ruchu DNS na podstawie następujących algorytmów:
3.5.1 cykliczna,
3.5.2 ważona,
3.5.3 najmniejsza liczba połączeń,
3.5.4 najszybsza odpowiedź serwera,
3.5.5 najmniejsza liczba połączeń i najszybsza odpowiedź serwera,
3.5.6 najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie,
3.5.7 dynamicznie ważona oparta na SNMP/WMI,
3.5.8 definiowana na podstawie grupy priorytetów dla serwerów,
3.5.9 musi istnieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego.
3.6 Rozwiązanie musi posiadać wbudowany w system operacyjny język skryptowy, posiadający co najmniej następujące cechy:
3.6.1 Analiza, zmiana oraz zastępowanie parametrów DNS,
3.6.2 Generowania odpowiedzi na podstawie zapytania DNS oraz stanu zapisanego w pamięci urządzenia (np. historyczne zapytania DNS od danego użytkownika),
3.6.3 Powinna istnieć możliwość nadpisania statycznych reguł kierowania ruchu, na podstawie dowolnych atrybutów żądania DNS, oraz stanu sesji zapisanego w pamięci urządzenia,

3.6.4 Język skryptowy powinien umożliwiać iteracje poprzez wszystkie rekordy odpowiedzi DNS, oraz odczytywanie, modyfikacje i usuwanie poszczególnych rekordów,
3.6.5 Język skryptowy powinien umożliwiać odczyt, modyfikacje i wstawienie sekcji additional,
3.6.6 Język skryptowy powinien umożliwiać odczyt i modyfikację:
3.6.6.1 Typu rekordu,
3.6.6.2 TTL,
3.6.6.3 Nazwy rekordu,
3.6.6.4 Klasy (class).
3.6.7 Język skryptowy powinien umożliwiać operacje porównania stringów: equals, contain, starts with, ends with,
3.6.8 Język skryptowy powinien wspierać REGEXP,
3.6.9 Język skryptowy powinien umożliwiać selektywne (per request) wyłączanie funkcji GSLB, DNS Resolver i Cache, autorytatywnego DNS,
3.6.10 Język skryptowy powinien umożliwiać selektywne (per request) wyłączanie funkcji GSLB, DNS Cache.

3.7 Powinna istnieć możliwość weryfikacji listy rekordów i reakcji / obsługi wyjątków, jeżeli domena lub zwracany adres IP znajduje się na liście.

3.8 Powinna istnieć możliwość zaimportowania i użyciu statycznej listy „wyjątków" powyżej 200 000 rekordów.

3.9 Powinna istnieć możliwość definiowania obsługi ruchu zarówno dla żądań jak i odpowiedzi DNS.

3.10 Rozwiązanie powinno pełnić funkcje serwera autorytatywnego.

3.11 Celem podwyższenia wydajności, zony statyczne powinny być ładowane do pomięci i obsługiwane z pamięci RAM.

3.12 Autorytatywny serwer DNS powinien działać zarówno jako primary/master jak i secondary/slave.

3.13 Rozwiązanie powinno wspierać zone transfer
3.13.1 obsługiwać TSIG,
3.13.2 inicjować transfer zony po otrzymaniu notyfikacji (NOTIFY),
3.13.3 Powinna istnieć możliwość przekazania notyfikacji do innych serwerów DNS.

3.14 Powinna istnieć możliwość definiowania nazw dla których jest implementowany mechanizm GSLB (Global Server Load Balancing).

3.15 Nazwy zwracające dynamiczne rekordy (GSLB) powinny nadpisywać statyczną definicje strefy (zony).

3.16 Mechanizm GSLB powinien obsługiwać następujące typy rekordów:
3.16.1 A,
3.16.2 AAAA,
3.16.3 CNAME,
3.16.4 MX,
3.16.5 NAPTR,
3.16.6 SRV.

3.17 Silnik GSLB powinien zwracać adresy IP do zasobów, które obsługują aplikacje z zapytania DNS. Adresy IP będą dalej nazywane serwerami virtualnymi.

3.18 Silnik GSLB powinien uwzględniać stan zasobów znajdujących się za adresami IP, do których może być skierowany użytkownik poprzez zwrócenie adresu IPv4 lub IPv6.

3.19 Stan zasobów powinien być wymieniany asynchronicznie pomiędzy:

3.19.1 Innymi autorytatywnymi serwerami DNS implementującymi GSLB,
3.19.2 Urządzeniami ADC (Application Delivery Controller) pochodzącymi od tego samego producenta,

3.20 Rozwiązanie powinno wspierać mechanizm Route Healt Injection (RHI),

3.21 Rozwiązanie GSLB powinno wspierać co najmniej następujące metody monitorowania:
3.21.1 http, https,
3.21.2 IMAP,
3.21.3 LDAP,
3.21.4 MSSQL, MySQL, PostgresSQL,
3.21.5 NNTP,
3.21.6 POP3,
3.21.7 RADIUS i RADIUS Accounting,
3.21.8 SIP,
3.21.9 SNMP,
3.21.10 SMTP,
3.21.11 SOAP,
3.21.12 TCP,
3.21.13 UDP,
3.21.14 Monitora skryptowego, definiującego sekwencje wymiany wiadomości
3.21.15 Monitora zewnętrznego, czyli uruchomienia procesu np. bash, perl, zwracającego stan zasobów na podstawie logiki zawartej w zewnętrznym programie / skrypcie.

3.22 Silnik GSLB powinien wspierać co najmniej następujące algorytmy load balancingu:
3.22.1 Cykliczna,
3.22.2 Ważona,
3.22.3 Na podstawie adresu IP resolvera, implementująca persystencji (przywiązywanie sesji),
3.22.4 Do pierwszego dostępnego virtualnego serwera, przy czym rozwiązanie powinno umożliwiać zdefiniowanie kolejności virtualnych serwerów,
3.22.5 Lokalizacji pytającego serwera, na podstawie zaszytej bazy geolokacyjnej.

3.23 Jeżeli wirtualny serwer jest zdefiniowany na urządzeniu ADC od tego samego producenta, silnik GSLB powinien wspierać co najmniej następujące algorytmy load balancingu:
3.23.1 Na podstawie wolnych zasobów procesora urządzenia ADC,
3.23.2 Ilości hopów pomiędzy LDNS a ADC,
3.23.3 Na podstawie aktualnego wysycenia połączeń do serwera wirtualnego, Mniejsze wysycenie oznacza większe prawdopodobieństwo wyboru,
3.23.4 Aktualnej ilości obsługiwanych połączeń przez ADC,
3.23.5 Pakietów na sekundę,
3.23.6 Round Trip Time,
3.23.7 Subiektywnej oceny wydajności przypisanej do wirtualnego serwera na urządzeniu ADC przez administratora,
3.23.8 Średniej ważonej z powyższych metryk.

3.24 Powinna istnieć możliwość grupowania obszarów geograficznych z dokładnością do poziomu województwa, tak aby zwiększyć prawdopodobieństwo połączenia Klienta z najbliższym CPD.

3.25 Powinna istnieć możliwość grupowania prywatnych adresacji w obszary i wykorzystania tych obszarów do algorytmu load balancingu.

3.26 Silnik GSLB powinien umożliwiać grupowanie zasobów / wirtualnych serwerów w Centra Przetwarzanie danych na podstawie ich rzeczywistej lokalizacji.

3.27 System GSLB powinien wspierać mechanizmy oceny dostępności Centrum Przetwarzania Danych.

3.28 W przypadku niedostępności Centrum Przetwarzania Danych, GSLB nie powinno zwracać adresów IP posadowionych w niedostępnym CPD, chyba że są one zdefiniowane statycznie.
3.29 Powinna istnieć możliwość delegacji procesu monitorowania wirtualnych serwerów posadowionych na rozwiązaniach firm trzecich do urządzenia ADC od tego samego dostawcy znajdującego się w tym samym CPD co wirtualne serwery.
3.30 Powinna istnieć możliwość delegacji procesu monitorowania wirtualnych serwerów, posadowionych na rozwiązaniach firm trzecich, do urządzenia ADC mającego routing do strefy, w której znajdują się monitorowane zasoby.
3.31 Powinna istnieć możliwość grupowania nazw, tak żeby dany klient był obsługiwany z tego centrum przetwarzania danych dla wszystkich nazw ze zdefiniowanego zbioru.
3.32 Rozwiązanie powinno wspierać trzy tryby pracy:
  3.32.1 Cache transparentny, gdzie cachowane są pełne odpowiedzi. W przypadku potrzeby rozwiązania zapytania (cache miss), cache transparentny przesyła zapytanie do drugiego poziomu cache-u,
  3.32.2 Resolvera z cachem,
  3.32.3 Resolvera walidującego podpisy DNS SEC z cachem.
3.33 Rozwiązanie powinno umożliwiać granularną konfigurację każdego typu cache'u, tak aby uzyskać optymalny stosunek czasu wyszukiwania rekordów do cache hit ratio. Rozwiązanie powinno umożliwiać strojenie przynajmniej następujących parametrów
  3.33.1 Dla cache-u transparentnego: dostępnej pamięci dla cachu wiadomości i cachu rekordów,
  3.33.2 W trybie pracy resolver z cachem: dostępnej pamięci dla cachu wiadomości, cachu rekordów i cachu autorytatywnych serwerów nazw,
  3.33.3 W trybie pracy resolver walidującego DNS SEC z cachem: dostępnej pamięci dla cachu wiadomości, cachu rekordów, cachu autorytatywnych serwerów nazw i cachu kluczy DNS SEC.
3.34 Resolver powinien zbierać i utrzymywać statystyki czasu odpowiedzi serwerów autoratywnych i wykorzystywać te statystyki w celu skrócenia czasu rozwiązywania nazw.
3.35 Rozwiązanie powinno wykorzystywać IPv4 i IPv6 do komunikacji z serwerami autorytatywnymi.
3.36 Rozwiązanie powinno umożliwiać przeszukiwanie cachowanych rekordów.
3.37 Rozwiązanie powinno umożliwiać selektywne usuwanie cachowanych rekordów.
3.38 System powinien filtrować w oparciu o Response Policy Zone.
3.39 System powinien filtrować w oparciu o pliki płaskie, gdzie w pliku płaskim do każdej domeny może być przypisana akcja, np. NX Domain, odpowiedź CNAME, A record itd.
3.40 Resolver powinien zbierać co najmniej następujące statystyki:
  3.40.1 Ilość zapytań,
  3.40.2 Odpowiedzi,
  3.40.3 Wykorzystanych autorytatywnych serwerów,
  3.40.4 Odpowiedzi wygenerowanych lokalnie,
  3.40.5 Trafień w Response Policy Zone,
  3.40.6 Trafień / nietrafień w cache, per typ cachu (cache wiadomości, resource rekord, autorytatywne servery),
  3.40.7 Wyników rozwiązywań zapytań, np. sukces, timeout, przepełnienie kolejki,
  3.40.8 Odpowiedzi ze strony serwerów autorytatywnych.
3.41 Statystyki powinny być dostępne za pomocą SNMP.
3.42 Powinna istnieć możliwość definiowania wyjątków dla zapytań trafiających do systemu resolvera, przynajmniej dla następujących przypadków:

3.42.1 Powinna istnieć możliwość przekazania zapytania dla predefiniowanych subdomen do pooli serwerów DNS odpowiedzialnych za te domeny,
3.42.2 Powinna istnieć możliwość przekazania zapytania dla predefiniowanych domen odwrotnych do pooli serwerów DNS odpowiedzialnych za te domeny odwrotne,
3.42.3 Generowania predefiniowanej odpowiedzi, jeżeli w oryginalnej odpowiedzi z serwera autorytatywnego znajdzie się IP adres o złej reputacji.

3.43 Silnik systemu (resolvera) powinien mieć możliwość skorzystania z bazy reputacyjnej adresów IP celem usuwania tychże adresów z odpowiedzi od serwera autorytatywnego.

3.44 Rozwiązanie powinno filtrować po dowolnej kombinacji następujących typów zapytań:
a, axfr, dnskey, isdn, mb, naptr, nsec3param, rrsig, sshfp , a6, caa, ds, ixfr, md, nimloc, null, rt, tkey , aaaa, cert, eid, key, mf, ns, nxt, sig, tsig , afsdb, cname, gpos, kx, mg, nsap, opt, sink, txt , any, dhcid, hinfo, loc, minfo, nsap-ptr, ptr, soa, wks , apl, dlv, hip, maila, mr, nsec, px, spf, x25 , atma, dname, ipseckey, mailb, mx, nsec3, rp, srv, zxfr.

3.45 Rozwiązanie powinno być odporne na ataki typu „Phantom domain attack”.

3.46 Rozwiązanie powinno być odporne na ataki typu Lock-up domain”.

3.47 Rozwiązanie powinno śledzić i ograniczać
3.47.1 Liczbę pakietów o nieprawidłowej składni,
3.47.2 Liczbę pakietów per typ zapytania: A, PTR, NS, SOA, CNAME, MX, AAAA, TXT, SRV, AXFR, IXFR, ANY, NXDOMAIN, niemieszczących się w powyższych kategoriach,
3.47.3 Występowanie ataków typu reflection.

3.48 System musi posiadać moduł analizy ruchu DNS. Moduł powinien zbierać następujące metryki:
3.48.1 Typy zapytań,
3.48.2 Domeny,
3.48.3 Najaktywniejsi Klienci per IP, Kraj,
3.48.4 Typy ataków,
3.48.5 Wektory ataków.

3.49 Dla funkcjonalność GSLB system musi realizować co najmniej następujące funkcjonalności:
3.49.1 Global Server Load Balancing,
3.49.2 Dynamiczne podpisywanie domen DNS SEC,
3.49.3 DNS Caching,
3.49.4 Walidacja podpisów odpowiedzi DNS SEC,
3.49.5 Rozkład ruchu pomiędzy serwerami DNS innych producentów,
3.49.6 Ochrona przed atakami DDoS na protokół DNS,
3.49.7 Ochrona przed atakami DDoS na niższe (niż DNS) protokoły w modelu ISO/OSI.

3.50 Rozwiązanie powinno wspierać cache transparentny, gdzie cachowane są pełne odpowiedzi. W przypadku potrzeby rozwiązania zapytania (cache miss), cache transparentny przesyła zapytanie do drugiego poziomu cache-u.

3.51 Rozwiązanie powinno umożliwiać granularną konfigurację cache’u, tak aby uzyskać optymalny stosunek czasu wyszukiwania rekordów do cache hit ratio. Rozwiązanie powinno umożliwiać strojenie dostępnej pamięci dla cachu wiadomości i cachu rekordów.

4. Moduł uwierzytelniania użytkowników do aplikacji oraz SSL VPN musi posiadać co najmniej następujące funkcje:

4.1 System musi mieć wsparcie dla następujących metod uwierzytelniania użytkowników w dostępie do systemów:

- 4.1.1 Lokalna baza użytkowników – bez odwoływania się do zewnętrznych systemów
  certyfikatów cyfrowych
- 4.1.2 LDAP / LDAPS
- 4.1.3 SAML 2.0 - Security Assertion Markup Language
  Kerberos SSO/ NTLM
- 4.1.4 RSA SecureID
- 4.1.5 Radius
- 4.1.6 TACACS - Terminal Access Controller Access-Control System
  OAuth / OpenID
- 4.1.7 wbudowany w rozwiązanie mechanizm generowania (bez wysyłania) jednorazowych kodów OTP
- 4.1.8 OCSP Responder
- 4.1.9 Obsługę dla SSO pomiędzy wieloma domenami
- 4.1.10 Obsługę SAML 2.0 w trybach IDP oraz SP
- 4.1.11 Obsługę dedykowanych tuneli aplikacyjnych per aplikacja
- 4.1.12 Dynamiczną kontrolę dostępu użytkowników
- 4.1.13 Dynamiczne portale bazujące na tożsamości użytkownika

4.2 Moduł SSL VPN musi posiadać co najmniej następujące funkcje:

- 4.2.1 Obsługa tuneli szyfrowanych SSL VPN z pomocą dedykowanego klienta lub w przypadku dostępu przez przeglądarkę, dodatkowego komponentu do systemu operacyjnego
- 4.2.2 Obsługa IPv6
- 4.2.3 Moduł SSL VPN musi obsługiwać tryb wymuszający nawiązanie połączenia VPN, tzw. tryb always-on dla systemu Windows
- 4.2.4 Wsparcie dla zewnętrznego uwierzytelnienia w dostępie SSL VPN tzw. captive portal
- 4.2.5 System musi umożliwiać kompresję przesyłanych danych
- 4.2.6 Możliwość sprawdzania stacji końcowej pod kątem bezpieczeństwa
  - 4.2.6.1 Sprawdzanie obecności pliku w systemie
  - 4.2.6.2 Sprawdzanie aktywnego procesu w systemie
  - 4.2.6.3 Sprawdzanie aktywnego systemu antywirusowego, antyspareware
  - 4.2.6.4 Sprawdzanie stanu Firewalla systemowego
  - 4.2.6.5 Sprawdzanie zainstalowanych poprawek systemowych
  - 4.2.6.6 W przypadku systemu Windows sprawdzanie wpisu do rejestru systemowego
  - 4.2.6.7 Sprawdzanie certyfikatu
  - 4.2.6.8 Sprawdzanie informacji o zasobach hardware urządzenia klienta
- 4.2.7 System musi umożliwiać dynamic split-tunneling

4.3 Moduł SSL VPN musi posiadać mechanizm raportowy, uwzgledniający nie mniej niż:

- 4.3.1 Błędne próby uwierzytelnienia
- 4.3.2 Informacje o użytkownikach
- 4.3.3 Zasoby, do których odwołują się użytkownicy

4.3.4 Geolokalizację użytkownika

4.4 System musi zapewniać obsługę nie mniej niż 500 jednocześnie pracujących użytkowników SSL VPN z możliwością licencyjnej rozbudowy do 20 tysięcy licencji.

4.5 System musi zapewniać obsługę sesji uwierzytelniania typu

4.5.1 Microsoft Exchange

4.5.2 Outlook Anywhere, ActiveSync, Web Service

4.5.3 Microsoft OWA (without a rewrite profile)

4.5.4 WebAuth

4.5.5 SAML

4.6 Licencjonowanie musi odbywać się per ilość jednocześnie pracujących użytkowników z możliwością instalacji klienta SSL VPN na dowolnej ilości urządzeń/stacji roboczych.

4.7 System musi umożliwiać metody dostępu poprzez

4.7.1.1 Portal użytkownika z funkcjonalnością SSO (webtop)

4.7.1.2 Tunelu aplikacyjnego

4.7.1.3 Dostępu sieciowego (VPN)

4.7.2 Obsługa Microsoft ActiveSync i Outlook Anywhere z client-side NTLM

4.7.3 Listy dostępu (ACL) dla warstwy 7 modelu OSI

4.7.4 Buforowanie poświadczeń oraz SSO proxy

4.7.5 Zewnętrzne strony logowania

4.7.6 Obsługa wielu platform użytkowników (iPadOS, IOS, MacOS, Windows, Linux, Android)

4.7.7 Obsługa OAuth i OAuth 2.0

4.7.8 Obsługa JSON Web Token (JWT) z OAuth

4.7.9 Obsługa Google reCAPTCHA V2

4.7.10 Obsługa WebSockets dla dostępu przez portal

4.7.11 Obsługa integracji z ADFS Proxy (PIP)

4.7.12 Integracja z MS Intune Device, Airwatch, MAAS360 dla wyniku weryfikacji stanu urządzeń końcowych

4.7.13 Obsługa OpenID Connect Support dla OAuth Resource Server i Client

4.7.14 Obsługa serwera uwierzytelnienia dla OpenID Connect

4.7.15 Konfiguracja proxy Identity-aware dla architektur Zero Trust. System musi realizować dynamiczną zmianę polityki bezpieczeństwa odpowiadającą zmianie warunków dostępu użytkownika

4.7.16 System musi umożliwiać content i URL rewriting podczas bezagentowego dostępu do zasobów wewnętrznych w trybie reverse proxy

4.7.17 Obsługa walidacji dla modelu Zero Trust:

4.7.17.1 Tożsamości użytkownika

4.7.17.2 Wynik kontroli bezpieczeństwa urządzenia

4.7.17.3 MFA (multifactor authentication)

4.7.18 Integracja z IDaaS

4.7.19 Możliwość integracji z systemami AAA firm trzecich za pomocą wywołań API

4.7.20 Wsparcie dla FIDO U2F via API (YubiKey)

4.7.21 Wsparcie dla DTLS 1.2 dla klienta VPN

4.7.22 Wsparcie dla Microsoft Conditional Access rules (Azure AD)

4.7.23 Obsługa OpenAPI 3.0 dla importu polityki bezpieczeństwa API w ramach AuthZ/AuthN

4.7.24 Dynamiczny Split Tunneling (Zoom, Office 365)

4.7.25 Obsługa dla OpenID Connect protocol dla Duo MFA

4.7.26 Wsparcie dla Microsoft Identity Platform 2.0

4.7.27 Graficzny interfejs umożliwiający budowanie reguł dostępowych

4.7.28 Obsługa języka skryptowego opartego na języku TCL lub równoważnym

4.7.29 System musi posiadać funkcję definiowania i edycji szablonów konfiguracji aplikacji. Szablony powinny służyć do optymalizacji procesu wdrażania systemu zarówno dla znanych aplikacji biznesowych, jak i własnych aplikacji klienta. W ramach opisanych szablonów musi istnieć możliwość automatycznej kontroli poszczególnych elementów konfiguracji szablonu i zabezpieczenie ich przed modyfikacją i usunięciem.

5. Web Application Firewall musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji Web. Firewall aplikacyjny musi działać jednocześnie z wykorzystanie pozytywnego i negatywnego modelu bezpieczeństwa:

5.1 Pozytywny model bezpieczeństwa powinien kontrolować co najmniej:

5.1.1 wystąpienie URL-i, długość URL-i,

5.1.2 typ servleta występujący pod danym url-em – format komunikacji (http form, JSON, XML, GWT)

5.1.3 przejścia pomiędzy URL-ami (servletami)

5.1.4 dopuszczalne metody http,

5.1.5 dopuszczalne cookie,

5.1.6 dopuszczalne parametry w polityce,

5.1.7 parametry dynamiczne,

5.1.8 typ/format parametrów (alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML, e-mail, telefon, plik uploadowany)

5.1.9 dopuszczalne parametry w danym servlecie

5.1.10 długość zapytań

5.1.11 nazwy hosta

5.1.12 wystąpień i długość parametrów (per każdy parametr)

5.1.13 wystąpień i długości nagłówków

5.1.14 wystąpień i długości cookies

5.1.15 oczekiwanych typów znaków per każdy parametr

5.1.16 typów rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku URL-i podatnych na CSRF

5.2 Profil aplikacji web musi być tworzony na podstawie analizy ruchu sieciowego

5.3 WAF musi umożliwiać definiowania dopuszczalnego przepływu sekwencji zapytań w obrębie aplikacji z uwzględnieniem jej logiki biznesowej

5.4 Tworzenie profilu bezpieczeństwa Web Application Firewall dla danej aplikacji musi odbywać się na podstawie analizy ruchu sieciowego w szczególności na podstawie publicznego ruchu produkcyjnego.

5.5 System musi posiadać funkcję definiowania i edycji szablonów konfiguracji aplikacji. Szablony powinny służyć do optymalizacji procesu wdrażania systemu zarówno dla znanych aplikacji biznesowych, jak i własnych aplikacji klienta. W ramach opisanych szablonów musi istnieć możliwość automatycznej kontroli poszczególnych elementów konfiguracji szablonu i zabezpieczenie ich przed modyfikacją i usunięciem.

5.6 Algorytmy tworzenia profilu bezpieczeństwa WAF powinny odrzucać próby ataków w procesie nauki.

5.7 Musi istnieć możliwość definicji zaufanych adresów źródłowych, z których algorytm tworzenia profilu bezpieczeństwa WAF będzie akceptować wszystkie zachowania jako prawidłowe, tak aby administrator mógł przyspieszyć proces tworzenia profilu bezpieczeństwa.

5.8 Musi istnieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki bezpieczeństwa

5.9 Musi istnieć możliwość ochrony dynamicznych oraz ukrytych parametrów zapytań http

5.10 WAF musi automatycznie wykrywać false positive i wyłączać odpowiadające nim sygnatury dla danego parametru

5.11 WAF musi posiadać funkcjonalność automatycznego wykrywania stron logowania użytkowników oraz automatycznie włączać dla tych stron ochronę przed atakami brute force.

5.12 Mechanizm zabezpieczenia przed manipulacją cookie serwera aplikacyjnego powinien być oparty o wstrzykiwanie cookie z podpisem oryginalnego cookie aplikacji.

5.13 WAF powinien chronić przed kradzieżą sesji poprzez porównywanie „odcisku palca" (fingerprint) przeglądarki z sesją użytkownika. Mechanizm musi działać także dla TLS (TLS fingerprintig)

5.14 Mechanizm zabezpieczenia przed Cross-Site Request Forgery powinien dodawać losowy token do odpowiedzi http zawierających odwołania do chronionego zasobu (servleta).

5.15 System musi zapewniać możliwość wyboru polityki bezpieczeństwa na podstawie: Host, URL, Nagłówków, Cookie

5.16 Oprócz pozytywnego modelu zabezpieczeń WAF musi posiadać również funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń)

5.17 WAF musi posiadać mechanizmy ochrony przed atakami: Broken Access Control, SQL Injection, Cross-Site Scripting, Cross-Site Request Forgery, Session hijacking, Command Injection, Cookie/Session Poisoning, Parameter/Form Tampering, Forceful Browsing, Brute Force Login, Web Scraping, Cookie manipulation/poisoning, Dynamic Parameter tampering, Buffer Overflow, Stealth Commanding, Unused HTTP Methods, Malicious File Uploads, Hidden Field Manipulation

5.18 Musi istnieć możliwość selektywnego włączania/wyłączania sygnatur per parametr

5.19 Dla każdej chronionej aplikacji internetowej urządzenie powinno umożliwiać wybór stosowanych technologii i systemu operacyjnego w celu poprawnego doboru wykorzystywanych sygnatur uwzględniając, ale nie ograniczając się do:

- 5.19.1 Bazy danych: ORACLE, MySQL, Microsoft SQL Server, PostgreSQL, Sybase, IBM DB2, CouchDB, Elasticsearch, MongoDB, SQLite, Sybase/ASE
- 5.19.2 System Operacyjny: Windows, Linux, UNIX
- 5.19.3 Język aplikacji, frameworki, biblioteki: ASP, ASP.NET, PHP, Java Servlets, JavaScript, AngualrJS, Backbone.js, CodeIgniter, Django, Java Server Faces, BEA WebLogic, CGI, Elasticsearch, Front Page Server

Extension, Lotus Domino, Macromedia ColdFusion, Outlook Web Access, SSI, WebDAV, jQuery, SSI, Apache Struts, ef.js, Ember.js, Express.js, GraphQL, Handlebars, JavaServer Faces, Laravel, MooTools, Moustache, Python, React, RequireJS, Ruby, Spring Boot, UIKit, Underscore.js, Vue.js, WebDAV, Zend, ZURB Fundation

5.19.4 Serwer WWW, silniki: Apache, Apache Tomcat, Microsoft IIS, serwerów proxy, Jenkins, Jetty, Joomla, Macromedia JRun, Nginx, Node.js, Oracle Application Server, Oracle Identity Manager, Redis, Typo3 CMS

5.20 WAF musi posiadać mechanizmy ochrony przed atakami DoS ukierunkowanymi na warstwę aplikacyjną (np. Slow Loris, http Smuggling)

5.21 WAF musi rozróżniać rzeczywistych użytkowników od automatów podczas ataku (D)DoS poprzez:

5.21.1 Wstrzykiwanie skryptu JavaScript i weryfikacji rezultatów jego wykonania

5.21.2 Mechanizmu browser fingerprinting, w celu wykrycia tzw. headless broser

5.21.3 Sygnatur botów

5.21.4 Wykorzystanie CAPTCHA (tylko w przypadku, gdy powyższe mechanizmy nie rozstrzygają czy podłączony jest rzeczywisty użytkownik).

5.22 System powinien umożliwiać proaktywne wykrywanie i blokowanie botów (j.w.), zanim wywołają atak DDoS, web scraping lub brute force.

5.23 System musi rozróżniać ruch generowany przez boty za pomocą zasobów lokalnych

5.24 System musi posiadać możliwość rozbudowy licencyjnej o wysyłanie części ruchu do dalszej analizy w scrubbing center, w celu ochrony przed botami

5.25 WAF musi zawierać moduł sztucznej inteligencji, który na bieżąco obserwuje ruch od użytkowników końcowych, celem budowy i utrzymania modelu prawidłowego ruchu do aplikacji. WAF na podstawie behawioralnej analizy ruchu bieżącego i zbudowanego modelu, powinien wykrywać i chronić aplikację przed atakiem DDoS w warstwie 7. W systemie nie może być żadnego licencyjnego limitu dla tej funkcji.

5.26 System powinien kategoryzować boty i umożliwiać przepuszczanie ruchu od pożytecznych botów (np. search enginy), blokując ruch od szkodliwych botów.

5.27 Moduł ochrony przed DDoS powinien wykrywać ataki per:Source IP, Urządzenie, na bazie „odcisku palca” urządzenia, Obszar geolokacyjny, URL, Globalnie – website

5.28 Powinna istnieć możliwość przypisania różnych poziomów detekcji ataków (D)DoS dla danych URL-i portala. Np. /infoportal/* powinien posiadać luźniejszą politykę detekcji i zapobiegania ataków DDoS niż /portal/*.

5.29 System powinien wykrywać i chronić przed atakami DDoS na tzw. ciężkie servlety, czyli takie wywołujące złożone operacje obliczeniowe np. skomplikowane zapytania do baz danych.

5.30 Wykrycie ataku na ciężkie servlety powinno opierać się przynajmniej o ilość zapytań (TPS) oraz czas odpowiedzi

5.31 System powinien umożliwiać definicję maksymalnego czasu próbki ruchu, maksymalnej pojemności próbki ruchu, interwału czasowego pomiędzy pobieraniem próbki ruchu.

5.32 System powinien umożliwiać automatyczny zapis przykładowego ruchu do plików zgodnych z formatem TCP dump, w momencie wykrycia ataku (D)DoS.

5.33 Powinna istnieć możliwość doboru odpowiedzi w zależności do rodzaju naruszenia

5.34 WAF musi posiadać możliwość uwzględniania w logach dotyczących incydentów informacji o uwierzytelnionym użytkowniku oraz blokowania określonej liczby incydentów wykonywanych w zdefiniowanym czasie przez tego użytkownika.

5.35 WAF powinien umożliwiać usuwanie nagłówków serwera aplikacyjnego zdradzających technologię oraz wersję oprogramowania; bez uszczerbku na wydajności WAF-a.

5.36 WAF powinien umożliwiać wstrzykiwanie nagłówków np. w celu ochrony przed Clickjack-iem

5.37 WAF powinien umożliwiać podmianę kodów statusów zwracanych przez serwer aplikacyjny

5.38 W obrębie licencji WAF dostarczony musi być moduł ochrony protokołu HTTP, SMTP oraz FTP DNS, API

5.39 WAF musi mieć możliwość wgrania pliku swagger file (Open API) w celu budowy polityki typu whitelist dla API

5.40 WAF musi posiadać wsparcie dla aplikacji AJAX oraz JSON.

5.41 WAF powinien wyświetlać stron blokowania (błędu) w technologiach AJAX i JSON

5.42 WAF musi posiadać wsparcie dla Google Web Toolkit

5.43 WAF musi posiadać wsparcie dla GraphQL

5.44 WAF musi posiadać możliwość ochrony komunikacji XML poprzez:

- 5.44.1 walidację Schema/WSDL,
- 5.44.2 wybór dozwolonych metod SOAP,
- 5.44.3 szyfrację /deszyfrację fragmentów wiadomości SOAP,
- 5.44.4 wsparcie dla WS-Security (szyfracja, deszyfracja, veryfikacja i podpisywanie),
- 5.44.5 definiowanie możliwości użycia załączników wiadomości SOAP,
- 5.44.6 włączanie/wyłączanie podążania za odnośnikami do schematów SOAP,
- 5.44.7 walidację SOAP Action Header,
- 5.44.8 włączanie/wyłączanie możliwości użycia DTD
- 5.44.9 włączanie/wyłączanie możliwości użycia zewnętrznych referencji
- 5.44.10 włączanie/wyłączanie możliwości użycia początkowych białych znaków
- 5.44.11 włączanie/wyłączanie możliwości użycia numerycznych nazw
- 5.44.12 włączanie/wyłączanie możliwości użycia Processing Instructions
- 5.44.13 włączanie/wyłączanie możliwości użycia CDATA
- 5.44.14 ograniczenie długości: dokumentu, elementu, nazwy, wartości atrybutu, Namespace
- 5.44.15 ograniczenia ilości: zagnieżdżeń w dokumencie, dzieci per element, atrybutów per element, deklaracji NameSpace-ów
- 5.44.16 definicję dopuszczalnych znaków
- 5.44.17 definicję sygnatur.

5.45 WAF musi umożliwiać blokowanie zapytań z danego obszaru geograficznego. Aktualizacje bazy geolokacyjnej powinny być dostępne w ramach podstawowych opłat wsparcia.

5.46 WAF musi umożliwiać automatyczne budowanie polityk w oparciu o skanowanie przez zewnętrznych dostawców (przynajmniej trzech) np. Cenzic, HP WebInspect, IBM AppScan, Qualys Guard, WhiteHat Sentinel.

5.47 WAF musi posiadać mechanizmy normalizacji w celu obrony przed technikami ukrywania ataku. Mechanizmy normalizacji muszą wspierać/wykrywać:

- 5.47.1 Directory traversal
- 5.47.2 Kodowanie typu %u
- 5.47.3 Kodowanie typu IIS backslash
- 5.47.4 IIS Unicode codepoints
- 5.47.5 Bare byte decoding
- 5.47.6 Apache whitespace
- 5.47.7 Bad unescape
- 5.47.8 Wstrzykiwanie komentarzy (np. <!-- -->)

5.48 Mechanizm normalizacji powinien umożliwiać definiowanie maksymalnego zagnieżdżonego kodowania.

5.49 Urządzenie musi wspierać następujące tryby pracy:

- 5.49.1 Tryb wykrywania, logowania i blokowania ataków
- 5.49.2 Tryb wykrywania i logowania ataków bez blokowania
- 5.49.3 Tryb uczenia się bez blokowania
- 5.49.4 Tryb uczenia się z blokowaniem i logowaniem

5.50 WAF w trybie nauki, musi umożliwiać automatyczne, stopniowe przełączanie polityki bezpieczeństwa w tryb blokowania, np. servlety/parametry, dla których został zaobserwowany wystarczający ruch dla algorytmu nauki, zostaną przełączone w tryb blokowania, podczas gdy pozostałe pozostaną w trybie transparentnym.

5.51 WAF musi umożliwiać integracje systemami antywirusowymi po protokole ICAP w celu wykrywania wirusów w przesyłanych plikach.

5.52 WAF musi wykrywać i maskować numery kart kredytowych, wyciekających z chronionej aplikacji; oraz dowolnie inny ciąg znaków zdefiniowany poprzez PCRE regular expression.

5.53 WAF musi chronić ruch przesyłany po IPv6 bez degradacji wydajności wynikającej z innych czynników niż różnice protokołów IPv4 i IPv6

5.54 System musi umożliwiać szyfrowanie wskazanych pół (np. pole do wprowadzania danych typu hasło) w czasie rzeczywistym, wprowadzanym w przeglądarce internetowej.

5.55 Szyfrowanie musi być również dostępne, jeżeli formularz logowania wykorzystuje technologię AJAX. Szyfrowanie tych pól musi odbywać się z wykorzystaniem klucza publicznego osadzanego przez rozwiązanie w odpowiedzi serwera aplikacyjnego. System nie może wymagać zmiany po stronie samej aplikacji ani wymagać instalacji dodatkowego oprogramowania na urządzeniu końcowym.

5.56 System musi umożliwiać szyfrowanie w czasie rzeczywistym nazw wskazanych pól w kodzie HTML oraz dodawać dodatkowe pola typu input, by strona logowania www nie była statyczna (dodawanie dodatkowych pól typu input musi być niewidoczne dla użytkownika końcowego na stronie www).

6. Dla każdego z dostarczonych urządzeń należy dostarczyć 3 letnią subskrypcję dla serwisu reputacyjnego.

6.1 Serwis reputacyjny powinien być dostępny jako rozszerzenie systemu, bez konieczności wprowadzania zmian w architekturze sprzętowej oraz programowej proponowanego rozwiązania.

6.2 Serwis reputacyjny musi realizować co najmniej następujące funkcje:

6.2.1 Automatyczna aktualizacja informacji o zagrożeniach nie rzadziej niż co 5 minut

6.2.2 Rozpoznawać i blokować komunikację dla minimum poniższych:

6.2.2.1 Anonimowych proxy

6.2.2.2 Sieci Botnet

6.2.2.3 Aktywnych źródeł usług oferujących lub dystrybuujących malware, rootkity, robaki oraz wirusy

6.2.2.4 Źródeł ataków DDoS/DoS

6.2.2.5 Źródeł Exit Node sieci Tor

6.2.2.6 Adresów IP zainfekowanych przez malware

6.2.2.7 Adresów IP świadczących usługi hostingowe dla phishingu lub fraudów.

6.2.2.8 Źródeł ataków cross-site scripting, iFrame injection, SQL injection, cross domain injection czy domain password brute force

6.2.2.9 Źródłowych adresów IP skanerów służących do rekonesansu poprzez skanowanie hostów oraz domen

7. Dla każdego z dostarczonych urządzeń należy dostarczyć 3 letnią subskrypcję dla serwisu z sygnaturami aktualnych kampanii zagrożeń w Internecie.

7.1 Subskrypcje na sygnatury kontekstowe powiązane z konkretną kampanią ataków

7.2 Serwis sygnatur z aktualnymi kampaniami musi realizować następujące funkcje i informacje:

7.2.1 Natychmiastowa aktualizacja sygnatur z aktualnymi kampaniami

7.2.2 Musi dostarczać informacji o:

7.2.2.1 powiązaniu z konkretnym aktorem stojącym za atakami

7.2.2.2 wektorze ataku lub wykorzystanej technice

7.2.2.3 intencji ataku

7.2.2.4 datach dotyczących pierwszej obserwacji ataku, ostatnio widzianego ataku

7.2.2.5 statusie kampanii

7.2.2.6 analizie wykorzystanego payloadu

7.2.2.7 informacji o dodatkowych szkodach

8. Wysoka dostępność i analityka

8.1 System musi posiadać co najmniej następujące interfejsy administracyjne:

8.1.1 GUI przy wykorzystaniu protokołu https

8.1.2 Zarządzanie poprzez SSH

8.1.3 Zarządzanie poprzez API REST

8.2 System musi posiadać moduł analizy ruchu http. Moduł powinien zbierać następujące metryki

8.2.1 Czas odpowiedzi per serwer

8.2.2 Czas odpowiedzi per URI

8.2.3 Ilość sesji użytkownika
8.2.4 Przepustowość
8.2.5 Adres źródła
8.2.6 Kraj
8.2.7 User Agent (wykorzystywana przez klienta aplikacja)
8.2.8 Metoda dostępu

8.3 System musi posiadać następujące funkcje zarządzania siecią:
8.3.1 Obsługa protokołu SNMP v1/v2c/v3
8.3.2 Możliwość budowania własnych zdarzeń SNMP z własnymi numerami OID
8.3.3 Zewnętrzny syslog
8.3.4 Możliwość wysyłania logów syslog do więcej niż jednego miejsca docelowego
8.3.5 Zbieranie danych i ich wyświetlanie
8.3.6 Zbieranie danych zgodnie z ustawieniami administratora
8.3.7 Osobna brama domyślna dla interfejsu zarządzającego
8.3.8 Wsparcie dla przynajmniej 2 wersji oprogramowania (multi-boot)
8.3.9 zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy)
8.3.10 Dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu systemu.

8.4 System musi umożliwiać weryfikację działającego na urządzeniu firmware, czy nie uległ on modyfikacji (TPM Chain of Custody).

8.5 System musi posiadać funkcję integracji z zewnętrznymi serwerami uwierzytelnienia użytkowników LDAP, RADIUS, TACACS.

8.6 Autoryzacja administratorów systemu musi bazować na rolach użytkowników.

8.7 System musi posiadać funkcję definiowania i edycji szablonów konfiguracji aplikacji. Szablony powinny służyć do optymalizacji procesu wdrażania systemu zarówno dla znanych aplikacji biznesowych, jak i własnych aplikacji klienta.

8.8 Rozwiązanie musi oferować podział na tzw. partycje administracyjne. Zdefiniowany użytkownik może zarządzać konfiguracją tylko i wyłącznie wewnątrz swojej partycji.

8.9 Rozwiązanie musi oferować wsparcie dla tzw. domen routingu (Virtual Routing and Forwarding). Rozwiązanie takie oferuje separację ruchu sieciowego do różnych aplikacji. Musi umożliwiać poprawnie działanie rozwiązania, kiedy podłączone VLANy do urządzenia mają takie same podsieci i adresy IP.

8.10 Rozwiązanie musi oferować stworzenie minimum 1000 partycji administracyjnych oraz 1000 jednoczesnych domen routingu. Partycje administracyjne i domeny routingu muszą być dostępne również, jeżeli urządzenie pracuje w formie klastra.

8.11 Klaster wysokiej dostępności (HA) umożliwiający pracę w trybie active – standby powinien mieć możliwość realizacji również trybu active-active oraz rozbudowy do klastra N+1.

8.12 W ramach klastra musi istnieć możliwość jednoczesnego wykorzystania różnych modeli urządzeń sprzętowych oraz maszyn wirtualnych.

8.13 Klaster wysokiej dostępności musi zapewniać kopiowanie informacji o sesji SSL i stanu sesji TCP pomiędzy urządzeniami, aby uniknąć ponownej negocjacji po przełączeniu ruchu.

8.14 Klaster wysokiej dostępności musi zapewniać synchronizację:
- 8.14.1 Konfiguracji
- 8.14.2 Stanu połączeń
- 8.14.3 Przywiązywania sesji (Session persistence)
- 8.14.4 Polityk bezpieczeństwa aplikacyjnego

8.15 Wykrycie awarii urządzeń w klastrze odbywać się musi przy użyciu, co najmniej następujących metod:
- 8.15.1 Weryfikacja stanu pracy urządzenia poprzez analizę aktywności w sieci (Network failover)

WYDAJNOŚĆ ROZWIĄZANIA:

Przepustowość pojedynczego urządzenia z włączonym modułem WAF i inspekcjonującymi ruch politykami WAF oraz terminacją SSL/TLS musi być nie niższa niż 7,4 Gbps. Parametry powinny być spełnione przy min. charakterystyce ruchu: dla ruchu TLS – AES128-SHA, z kluczem min. 2048b, dla ruchu L7 – min. 100 żądań L7 na jedno połączenie TCP z odpowiedzią min. 5kB (wszystkie warunki muszą być spełnione równocześnie).

Powyższe parametry muszą zostać potwierdzone w oficjalnej dokumentacji producenta lub raportu z przeprowadzonych testów wydajnościowych udostępnionego na żądanie Zamawiającego.

Pozostałe parametry techniczne pojedynczego urządzenia zostały opisane w Tabela nr1.

Tabela nr1

	Pamięć RAM	Nie mniej niż 128 GB
	Przestrzeń dyskowa	1 x 1TB SSD
	Przepływność dla warstwy 4	Nie mniej niż 95 Gbps
	Przepływność dla warstwy 7	Nie mniej niż 60 Gbps, licencyjna możliwość aktualizacji do 95 Gbps
	Ilość transakcji SSL na sekundę dla klucza o długości 2048	Nie mniej niż 60 tysięcy, licencyjna możliwość aktualizacji do 100 tysięcy
	Ilość transakcji SSL na sekundę dla szyfru ECDSA P-256	Nie mniej niż 30 tysięcy, licencyjna możliwość aktualizacji do 70 tysięcy
	Przepływność ruchu szyfrowanego	Nie mniej niż 35 Gbps, licencyjna możliwość aktualizacji do 50 Gbps

	Ilość połączeń na sekundę w warstwie 4	Nie mniej niż 1 milion, licencyjna możliwość aktualizacji do 1 miliona 800 tysięcy
	Kompresja sprzętowa	Nie mniej niż 35 Gbps, licencyjna możliwość aktualizacji do 50 Gbps
	Ochrona sprzętowa przed atakami DDOS	Nie mniej niż 80 milionów SYN Cookies na sekundę
	Liczba vCPU dla wirtualnych instancji	Nie mniej niż 12, licencyjna możliwość aktualizacji do 26 vCPU
	Gęstość interfejsów	Nie mniej niż: • dwa interfejsy z możliwością obsadzenia wkładkami 100G QSFP28 lub 40G QSFP+, • osiem interfejsów z możliwością obsadzenia wkładkami 25G SFP28 lub 10G SFP+, • oddzielny port USB 3.0, • oddzielny port konsolowy, • oddzielny port zarządzania 1000 Base-T. Dla każdego z dostarczonych urządzeń powinny zostać dostarczone: • 2 wkładki 10G SR SFP+, Dopuszcza się tylko moduły w pełni wspierane przez producenta tego urządzenia.
	Zasilanie	Nie mniej niż dwa redundantne zasilacze - prąd zmienny 230V AC.

GWARANCJA I SERWIS:

Każde z urządzeń dostarczone przez Zamawiającego musi być objęte 3 letnią gwarancją producenta. W obrębie gwarancji zawarte musi być:

1.1 Dostęp do aktualnych wersji oprogramowania oraz dokumentacji producenta.
1.2 Sposób obsługi zgłoszeń gwarancyjnych w trybie 7x24.
1.3 Wymiana sprzętu następnego dnia roboczego po identyfikacji usterki.
1.4 W wypadku awarii dyski zostają u Zamawiającego.
1.5 Aktualizacja oprogramowania dostarczonych urządzeń przez Wykonawcę

USŁUGA DWROŻENIA U ZAMAWIAJĄCEGO

1. W ramach usługi wdrożenia Wykonawca dokona przeglądu konfiguracji urządzeń F5 serii i5800 posiadanych przez Zamawiającego, sporządzi projekt wymiany posiadanych przez Zamawiającego urządzeń na dostarczone przez Zamawiającego. Sporządzenie projektu będzie polegać na przeanalizowaniu konfiguracji posiadanych przez Zamawiającego urządzeń F5 serii i5800 wraz z konfiguracją urządzeń, które będą podłączone do dostarczonych urządzenia pod kątem poprawności konfiguracji, zgodności ze standardami obecnie stosowanymi przez producenta urządzeń. Wszystkie prace konfiguracyjne zostaną przeprowadzone w terminie ustalonym z Zamawiającym;
2. Zamawiającym po podpisaniu Umowy udostępni aktualną konfigurację posiadanych urządzeń sieciowych będących częścią wdrożenia a także pozostałych urządzeń których konfiguracja będzie niezbędna do poprawnego wykonania wdrożenia.
3. Wykonawca wykona usługę instalacji i konfiguracji dostarczonych Urządzeń i oprogramowania w miejsce posiadanych przez Zamawiającego w/w urządzeń firmy F5 serii i5800 w budynku O1 Polskiego Radia przy al. Niepodległości 77/85.
4. Instalacja musi być zaplanowana w sposób, który umożliwi jak najkrótszy czas niedostępności istniejącej sieci Zamawiającego.
5. Instalacja nastąpi po zaakceptowaniu przez Zamawiającego projektu migracji wykonanego przez Wykonawcę. Po zakończeniu prac, Wykonawca sporządzi dokumentację powykonawczą zawierającą aktualną konfigurację urządzeń wraz z opisem i rysunkami odwzorowującymi aktualną strukturę sieci.
6. Prace będą wykonywane na teranie Warszawy w godzinach uzgodnionych z Zamawiającym.

USŁUGA SZKOLENIA

1. Zamawiający wymaga voucherów na szkolenia dla trzech osób z zakresu zaoferowanych urządzeń i oprogramowania.
2. Szkolenia muszą odbyć się na terenie Polski, w certyfikowanym ośrodku producenta dostarczonych Urządzeń i Oprogramowania w ciągu 12 miesięcy od daty podpisania protokołu odbioru technicznego. Zamawiający dopuszcza formę szkolenia on-line (na odległość).
3. Zakresem szkolenia musi być architektura działania dostarczonych Urządzeń i sposób ich konfiguracji.
4. Szkolenia muszą być prowadzone przez instruktora w języku polskim.