Załącznik nr 1 do SIWZ

Szczegółowy opis przedmiotu zamówienia

Wymagania podstawowe dotyczące urządzeń do transmisji danych cyfrowych

I. Urządzenia do transmisji danych cyfrowych stanowią system bezpieczeństwa sieciowego

1. System bezpieczeństwa sieciowego składa się z następujących elementów:
    a) dwóch urządzeń pełniących funkcję bram bezpieczeństwa sieciowego działających w ramach klastra wysokiej dostępności active/standby wraz z zestawem odpowiednich licencji zapewniających ciągłość pracy w przypadku awarii jednego z urządzeń,
    b) jednego urządzenia pełniącego funkcję bezsygnaturowego wykrywania ataków zero-day poprzez analizę plików w wydzielonym środowisku wirtualnym,
    c) systemu zarządzania politykami bezpieczeństwa oraz konfiguracji urządzeń,
    d) systemu korelacji zdarzeń i raportowania.
2. Urządzenia muszą pochodzić od jednego producenta.
3. Autoryzowane szkolenie

W ramach wdrożenia należy przeprowadzić autoryzowane szkolenia producenta urządzenia dla 2 osób obejmujące swoim zakresem tematykę konfiguracji sprzętowej oraz tematykę konfigurację polityk bezpieczeństwa wszystkich zalicencjonowanych funkcjonalności. Szkolenie musi być oficjalnym szkolenie producenta ze ścieżki certyfikacyjnej typu professional.

II. Bramy bezpieczeństwa sieciowego

1. Wymagania ogólne

3.1. Bramy bezpieczeństwa sieciowego dostarczone muszą być w postaci dwóch urządzeń działających w ramach klastra wysokiej dostępności active/standby wraz zestawem odpowiednich licencji zapewniających ciągłość pracy w przypadku awarii jednego z urządzeń.

3.2. Oferowane urządzenia muszą umożliwiać uruchomienie następujących funkcjonalności dostarczonych przez jednego producenta:

a) Firewall,
b) IPS (ang. Intrusion Prevention System),
c) Zarządzanie identyfikacją użytkownika (ang. User Identity),
d) System automatycznego wykrywania i klasyfikacji aplikacji wraz z filtrowaniem URL,
e) Wykrywanie malware oraz komunikacji z serwerami C&C (wykrywanie urządzeń działających w sieci botnet),
f) Brama IPSec VPN,
g) Dostęp zdalny dla urządzeń mobilnych,
h) Zapewnienie możliwości uruchomienia w przyszłości ochrony przed wyciekiem informacji Data Loss Prevention poprzez dokupienie odpowiedniej licencji bądź wykupienie subskrypcji.

3.3. Oferowane urządzenia muszą być dostarczone wraz zestawem odpowiednich licencji oraz subskrypcji obejmujących dostęp do aktualizacji baz sygnatur przez okres 3 lat.

2. Wymagania sprzętowe

2.1 Urządzenia muszą być dostarczone w formie dedykowanej platformy sprzętowej (nie będącej serwerem ogólnego przeznaczenia).

2.2 Każde urządzenie musi być wyposażone przynajmniej w następujące interfejsy (wbudowane w urządzenie lub jako dodatkowe moduły):

1. 10 interfejsów 10/100/1000BASE-T RJ45,
2. 6 interfejsów 10GE SFP+ z czterema wkładkami typu LR o zasięgu 10km oraz co najmniej dwoma wkładkami typu SR o zasięgu 330m.

2.3 Urządzenie powinno charakteryzować się:

a) maksymalną wysokością wynoszącą 2U,
b) dostępną pamięcią RAM min. 32GB,
c) musi posiadać co najmniej dwa dyski twarde (HDD lub SSD) pracujące w konfiguracji RAID 1,
d) musi posiadać dwa redundantne zasilacze, zasilane prądem przemiennym 230V (niedopuszczalne musi być urządzenie zewnętrzne),

3. Funkcjonalności

Każde z dwóch urządzeń musi realizować podane poniżej funkcjonalności z podaną wydajnością:

3.1 Firewall

3.1.1 Urządzenie musi realizować inspekcję stanową opartą na granularnej analizie komunikacji oraz stanu aplikacji w celu poprawnego śledzenia i kontroli przepływu ruchu.

3.1.2 Urządzenie musi realizować inspekcję stanową z wydajnością nie mniejszą niż 30Gbps z możliwością uzyskania do 77Gbps dla pakietów 1518UDP (maksymalna osiągalna wydajność w warunkach testowych zgodnych z RFC 3511, 2544, 2647, 1242).

3.1.3 Urządzenie musi obsługiwać co najmniej 12 800 000 jednoczesnych sesji/połączeń z prędkością zestawiania co najmniej 185 000 połączeń na sekundę.

3.1.4 Urządzenie musi pozwalać na kontrolę przynajmniej 150 predefiniowanych serwisów/protokołów.
3.1.5 Urządzenie musi posiadać możliwość zaraportowania ilości „trafień" wybranej polityki do aplikacji zarządzającej.
3.1.6 Tworzenie reguł musi pozwalać na ich konfiguracje w określonych interwałach czasowych wraz z podaniem daty lub godziny ich wygaśnięcia.
3.1.7 Urządzenie musi posiadać możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (ang. Identity Firewall), integrując się usługą katalogową Microsoft Active Directory bądź inną implementacją protokołu LDAP.
3.1.8 Integracja z Microsoft Active Directory bądź inną implementacja protokołu LDAP nie może wymagać żadnego dodatkowego serwera, który pośredniczyłby w wymianie informacji z systemem zabezpieczeń.
3.1.9 Urządzenie musi posiadać lokalną bazę użytkowników pozwalającą na ich uwierzytelnianie bez potrzeby korzystania z zewnętrznych rozwiązań.
3.1.10 Urządzenie pracujące w klastrze wysokiej dostępności musi umożliwiać pracę w trybie Transparent/Bridge.
3.1.11 Urządzenie musi wspierać pracę w trybie wysokiej dostępność (HA) zapewniającą synchronizacją stanu sesji w tym sesji VPN (Remote Access i Site-To-Site). Urządzenia muszą zapewniać wsparcie dla pracy w trybie Active/Active oraz Active/Standby.
3.1.12 Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
3.1.13 Urządzenie musi realizować funkcję inspekcji ruchu SSL dla ruchu przychodzącego i wychodzącego, w tym zapewnia:
a) wsparcie dla Perfect Forward Secrecy (PFS, ECDHE),
b) wsparcie dla AES-NI i AES-GCM,
c) import certyfikatu z zewnętrznego CA,
d) administrator musi mieć możliwość definiowania reguł, które będą definiowały ruch który nie będzie podlegał dekrypcji SSL; w regułach tych można wykorzystać kategorie URL, w szczególności te dla bankowości elektronicznej.
3.1.14 Urządzenie musi umożliwiać komunikację z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS i TACACS+.
3.1.15 Urządzenie musi umożliwiać eksport informacji przez syslog.
3.1.16 Urządzenie musi wspierać eksport zdarzeń opartych o przepływy za pomocą protokołu NetFlow lub analogiczny.
3.1.17 Urządzenie musi być konfigurowalne przez CLI oraz interfejs graficzny.
3.1.18 Dostęp do urządzenia musi być możliwy przez SSH.
3.1.19 Urządzenie musi obsługiwać protokół SNMP 1/2/3.

3.2 Wsparcie dla IPv6

3.2.1 Urządzenie musi pozwalać na obsługę IPv6 przez moduł Firewall, Kontroli Aplikacji, Antymalware oraz Filtrowania URL.
3.2.2 Urządzenie musi wspierać NAT64 lub tunele 6 do 4.
3.2.3 Urządzenie musi zapewniać integrację z usługami katalogowymi poprzez IPv6.
3.2.4 Urządzenie musi raportować ruch IPv6 oraz prezentować tabele routingu dla IPv6.
3.2.5 Urządzenie powinno musi być zgodne z poniższymi RFC dotyczącymi IPv6:
a) RFC 1981 Path Maximum Transmission Unit Discovery for IPv6
b) RFC 2460 IPv6 Basic specification
c) RFC 2464 Transmission of IPv6 Packets over Ethernet Networks

d) RFC 4007 IPv6 Scoped Address Architecture
e) RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers – wsparcie dla tuneli 6w4
f) RFC 4291 IPv6 Addressing Architecture (które zastąpiło RFC1884)
g) RFC 4443 ICMPv6
h) RFC 4861 Neighbor Discovery
i) RFC 4862 IPv6 Stateless Address Auto-configuration

3.3 Intrusion Prevention System (IPS):

3.3.1 Urządzenie musi zapewniać skuteczność wykrywania zagrożeń i ataków na poziomie minimum 98% udokumentowany przez niezależne testy (np. NSS Labs).

3.3.2 Urządzenie musi posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez urządzenie).

3.3.3 Urządzenie musi umożliwiać pracę zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu).

3.3.4 Urządzenie musi umożliwiać i zapobiegać szerokiej gamie zagrożeń (np.: złośliwemu oprogramowaniu, skanowaniu sieci, atakom na usługi VoIP, próbom przepełnienia bufora, atakom na aplikacje P2P, zagrożeniom dnia zerowego, itp.).

3.3.5 Urządzenie musi umożliwiać wykrywanie modyfikacji znanych ataków.

3.3.6 Urządzenie musi zapewniać co najmniej poniższe sposoby wykrywania zagrożeń:
a) sygnatury ataków opartych na exploitach,
b) reguły oparte na zagrożeniach,
c) mechanizm wykrywania anomalii w protokołach,
d) inspekcję nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakresu protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu.

3.3.7 Urządzenie musi posiadać wiele możliwości reakcji na zdarzenia, co najmniej: monitorowanie, blokowanie ruchu zawierającego zagrożenia, zapisywanie pakietów.

3.3.8 Urządzenie musi posiadać możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności, takich jak uruchomione systemy operacyjne, uruchomione serwisy, otwarte porty w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności.

3.3.9 Urządzenie musi umożliwiać pasywne gromadzenie informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych.

3.3.10 Urządzenie musi zapewniać możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.

3.3.11 Urządzenie musi umożliwiać automatyczną inspekcję i ochronę dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji.

3.3.12 Urządzenie musi umożliwiać obronę przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu musi stosować mechanizm defragmentacji i składania strumienia danych.

3.3.13 Urządzenie musi zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą byś pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne.
3.3.14 Urządzenie musi umożliwiać definiowanie wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednoczenie.
3.3.15 Urządzenie musi umożliwiać detekcję ataków i zagrożeń opartych na protokole IPv6.
3.3.16 Urządzenie musi posiadać mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego.
3.3.17 Urządzenie musi pozwalać na objęcie ochroną protokołów SCADA.
3.3.18 Urządzenie musi pozwalać na ochronę protokołów VOIP.

3.4 Identyfikacja użytkownika (User Identity)

3.4.1 Urządzenie musi umożliwiać identyfikację użytkowników zdefiniowanych w usłudze Microsoft Active Directory lub innej implementacji protokołu LDAP.
3.4.2 Urządzenie musi pozwalać na identyfikację i uwierzytelnianie użytkowników dla zasobów nie związanych z domeną. Funkcja ma być realizowana w formie portalu www, przez który użytkownik identyfikuje się na urządzeniu. Portal ten musi być konfigurowalny - w szczególności musi istnieć możliwość jego polonizacji oraz zmiany logo.
3.4.3 Urządzenie musi posiadać dedykowanego agenta instalowanego na stacji końcowej pozwalającego na identyfikację użytkownika.
3.4.4 Urządzenie musi wspierać środowiska terminalowe przez instalację dodatkowego agenta.
3.4.5 Urządzenie musi integrować się z usługami katalogowymi oraz serwerami RADIUS.
3.4.6 Urządzenie nie może wpływać na działanie kontrolera domeny.

3.5 System automatycznego wykrywania i klasyfikacji aplikacji wraz z filtrowaniem URL

3.5.1 Baza znanych aplikacji musi zawierać nie mniej niż 2 500 pozycji.
3.5.2 Urządzenie musi pozwalać na tworzenie reguł zawierających wiele kategorii.
3.5.3 Urządzenie musi posiadać mechanizm ograniczenia użycia pasma.
3.5.4 Strona informująca o zablokowanym zasobie musi umożliwiać modyfikowanie jej przez administratora. Urządzenie musi wykrywać wersję językową systemu, który się łączy i na tej podstawie wyświetlić stroną z komunikatem w tym właśnie języku. Dodatkowo musi istnieć możliwość przekierowania użytkownika na inna stronę.
3.5.5 Urządzenie musi wspierać mechanizmy białych i czarnych list.

3.6 Wykrywanie malware oraz komunikacji z serwerami C&C

3.6.1 Urządzenie musi umożliwiać wykrycie oraz blokadę podejrzanego zachowania w chronionych segmentach sieci.
3.6.2 Wykrycie zdarzenia musi opierać na wielowarstwowej analizie (połączenie reputacji adresów URL, IP, czy DNS połączonych z analizą cech charakterystycznych dla botnetów).
3.6.3 Funkcjonalność musi umożliwiać zarządzanie z centralnej konsoli.
3.6.4 Funkcjonalność musi posiadać możliwość:
a) inspekcji archiwów zagnieżdżonych,
b) blokowania określonych typów plików bez inspekcji,
c) tworzenia szczegółowych wyjątków obejmujących użytkowników, sieci, pliki, adresy URL, sygnatury.
3.6.5 Urządzenie musi umożliwiać integrację systemu wykrywania malware oraz komunikacji z serwerami C&C z system do bezsygnaturowego wykrywania ataków zero-day dostarczanych przez tego samego producenta.

3.7 VPN

3.7.1 Urządzenie musi wspierać wewnętrzne oraz zewnętrzne ośrodki certyfikacji.

3.7.2 Urządzenie musi posiadać wsparcie dla:

a) IKEv1: AES-256 oraz SHA-384 dla fazy I oraz dla fazy II AES-GCM-256,
b) IKEv2 „Suite-B-GCM-128" i „Suite-B-GCM-256",
c) PFS z Grupą 20 (384-bit ECP) Diffiego-Hellmana.

3.7.3 Urządzenie musi wspierać site-to-site VPN w następujących topologiach:

a) każdy do każdego (full mesh),
b) gwiazda,
c) połącznie poprzez huby.

3.7.4 Urządzenie musi wspierać użytkownika korzystającego z trybu klienta VPN (IPSec oraz SSL) oraz clientless SSL VPN.

3.7.5 Urządzanie musi realizować funkcje SSL VPN. Urządzenie musi zostać dostarczone z licencją umożliwiającą realizację 50 jednoczesnych połączeń.

3.7.6 Funkcja SSL VPN musi realizować co najmniej poniższe funkcje:

a) weryfikacje stanu stacji podczas podłączenia co najmniej w zakresie:
   - zainstalowanego oprogramowanie antywirusowego
   - zainstalowanych najnowszych poprawek systemu operacyjnego
   - zainstalowanej wersji firewalla
   - weryfikacji wpisów w rejestrze
   - weryfikacji sumy kontrolnej i wielkości dowolnego pliku
   - procesu uruchomionego w systemie
b) dostęp do koncentratora SSL VPN musi być zrealizowany w technologii web-base oraz client-base,
c) system musi realizować dwuetapowe uwierzytelnienie np. po uwierzytelnieniu certyfikatem w drugim etapie następuje wysłanie hasła jednorazowego przez firewall,
d) dostęp do wybranych zasobów musi być realizowany na podstawie wyników analizy stacji,
e) musi być możliwość uruchomienia specjalnego wyizolowanego środowiska, które będzie separowało pracę użytkownika od bazowego systemu operacyjnego,
f) administrator musi mieć możliwość ograniczenia aplikacji jakie użytkownik będzie mógł uruchomić będąc podłączony tunelem VPN do Firewalla,
g) musi istnieć możliwość uruchomienia skryptu podczas logowania się użytkownika do koncentratora VPN.

3.7.7 Funkcja IPSec VPN musi uwierzytelniać użytkowników za pomocą:

a) hasła statycznego,
b) certyfikatu,
c) hasła jednorazowego RSA SecurID.

3.7.8 Klient VPN musi sam wznawiać połączenie w przypadku jego zerwania.

3.7.9 Musi istnieć możliwość modyfikacji ustawień split tunnelingu (cały ruch ma być kierowany do urządzenia i na nim ma podlegać dalszej inspekcji).

III. Urządzenie do wykrywania ataków zero-day

1. Funkcjonalność urządzenia

1.1. Urządzenie musi być dedykowanym rozwiązaniem do bezsygnaturowego wykrywania ataków zero-day poprzez analizę plików w wydzielonym środowisku wirtualnym.

1.2. Urządzenie musi wykonywać zaawansowaną analizę plików w środowiskach zwirtualizowanych przynajmniej dla podanych systemów operacyjnych i oraz wersji oprogramowania:

1.2.1. Systemy operacyjne

a) Windows XP
b) Windows 7 32bit
c) Windows 7 64bit
d) Windows 8.1 64bit

1.2.2. Oprogramowanie Microsoft Office:

a) Office 2003
b) Office 2007
c) Office 2010
d) Office 2013

1.2.3. Oprogramowanie Adobe

1.3. Urządzenie musi wykonywać zaawansowaną analizę przynajmniej dla podanych formatów plików:

a) pakiet MS Office (doc, docm, docx, dot, dotm, dotx, potm, potx, ppam, pps, ppsm, ppsx, ppt, pptm, pptx, sldm, sldx, rtf, xlam, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw)
b) pliki wykonywalne (exe, scr)
c) pdf
d) archiwa (bz2, CAB, gz, rar, seven-Z, tar, tgz, zip)
e) swf (flash)
f) jar (java)
g) PIF
h) CSV

1.4. Urządzenie musi monitorować zachowanie analizowanych plików przynajmniej w następujących rejonach: system plików, rejestr systemowy, procesy, połączenia sieciowe.

1.5. Urządzenie musi mieć możliwość dzielenia się informacjami o wykrytych złośliwych plikach z innymi użytkownikami tego rozwiązania za pośrednictwem dedykowanej chmury producenta.

1.6. Urządzenie musi umożliwiać inspekcję plików przesyłanych poprzez następujące protokoły: HTTP, HTTPS, SMTP oraz SMB/CIFS.

1.7. W przypadku wykrycia nowego złośliwego pliku system musi tworzyć lokalną sygnaturę, która umożliwi automatyczne wykrycie i zablokowanie pobierania tego pliku przy kolejnych próbach pobrania.

1.8. Urządzenie musi umożliwiać konfigurację akcji podejmowanej w stosunku do pobieranych plików przynajmniej w następującym zakresie:

a) Pobierany plik nie musi być blokowany, jego skanowanie wykonywane musi być w tle
b) Pobierany plik musi być blokowany do czasu zakończenia inspekcji

1.9. Urządzenie musi dawać możliwość emulacji plików przesyłanych w komunikacji SSL i TLS.

1.10. Administrator musi mieć możliwość edycji komunikatu na stronie www, który zostanie wyświetlony użytkownikowi w przypadku zablokowania pobieranego pliku.

1.11. Urządzenie musi dawać możliwość wygenerowania szczegółowego raportu z analizy dla wszystkich plików, które zostały poddane inspekcji.

1.12. Raport musi zawierać informacje na temat nieprawidłowej aktywności uruchomionego pliku w zakresie: systemu pików, rejestru systemowego, procesów, połączeń sieciowych oraz zawierać faktyczne zrzuty ekranu przedstawiające środowisko emulacyjne w momencie uruchomienia pliku.

1.13. Moduł dostarczania bezpiecznych plików musi wspierać co najmniej następujące formaty:

a) Pakiet Microsoft Office: doc, docm, docx, dot, dotm, dotx, potm, potx, ppam, pps, ppsm, ppsx, ppt, pptm, pptx, sldm, sldx, rtf, xla, xlam, xlm, xls, xlsb, xlsm, xll, xlsx, xlt, xltm, xltx, xlw
b) Pdf, fdf

1.14. Proces bezpiecznego dostarczania plików musi być realizowany na co najmniej dwa sposoby:
a) Konwersja do statycznego pliku pdf
b) Usuwanie treści aktywnej i zachowanie pierwotnego formatu plików

1.15. Urządzenie musi posiadać moduł antywirusowy umożliwiający sygnaturową analizę plików.

1.16. Urządzenie musi posiadać moduł wykrywający hosty komunikujące się z sieciami botnet.

2. Parametry urządzenia

2.1. Wydajność urządzenia nie może być niższa niż 100 000 unikalnych plików miesięcznie poddawanych analizie.

2.2. Przepustowość urządzenia w przypadku wdrożenia w trybie inline min. 700 Mbps.

2.3. Urządzenie musi posiadać zasoby umożliwiające uruchomienie przynajmniej ośmiu maszyn wirtualnych stanowiących środowisko emulacyjne dla analizowanych plików.

2.4. Urządzenie musi posiadać minimum 9 interfejsów 10/100/1000 BASE-T z możliwością rozbudowy do 17 interfejsów za pomocą modułu rozszerzeń.

2.5. Urządzenie musi być dostarczone z zestawem trzyletnich subskrypcji na moduł antywirusowy, moduł wykrywający hosty w sieci botnet oraz moduł zaawansowanej analizy plików.

IV. System zarządzania politykami bezpieczeństwa

1. Zarządzanie politykami bezpieczeństwa oraz konfiguracją urządzeń musi być realizowane z poziomu dedykowanego, dostarczonego systemu zarządzania.
2. System zarządzenia musi być dostarczony jako oprogramowanie zabezpieczeń wraz z systemem operacyjnym dostarczanym i wspieranym przez jednego producenta i możliwym do instalacji na serwerze ogólnego przeznaczenia bądź w postaci maszyny wirtualnej Vmware lub jako oprogramowanie zainstalowane bezpośrednio na bramach bezpieczeństwa sieciowego.
3. System zarządzania wraz z zarządzanymi modułami musi pracować w architekturze trójwarstwowej - moduł urządzeń bezpieczeństwa sieciowego, moduł zarządzania i interfejs graficzny GUI. Komunikacja pomiędzy urządzeniami bezpieczeństwa sieciowego i modułem zarządzania musi być szyfrowana i uwierzytelniona z użyciem certyfikatów cyfrowych. Dopuszcza się rozwiązanie, w którym moduł zarządzający znajduje się bezpośrednio na bramach bezpieczeństwa sieciowego.
4. Uwierzytelnianie administratorów musi odbywać się za pomocą haseł statycznych, haseł dynamicznych i certyfikatów cyfrowych. Musi istnieć możliwość definiowania szczegółowych uprawnień administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkowników).
5. System zarządzania musi posiadać wbudowany wewnętrzny urząd certyfikacji (CA) do wydania certyfikatów VPN. Zarządzanie politykami bezpieczeństwa oraz CA musi odbywać się z tej samej konsoli GUI.
6. Zarządzanie politykami bezpieczeństwa na urządzeniach bezpieczeństwa sieciowego funkcjonującymi w różnych miejscach sieci musi odbywać się z centralnej, graficznej konsoli administratora GUI. Konsola zarządzania musi posiadać możliwość automatycznej weryfikacji spójności i niesprzeczności wprowadzonej polityki bezpieczeństwa. Oznacza to, że przed implementacją polityk bezpieczeństwa na urządzeniach bezpieczeństwa sieciowego system musi sprawdzić ich spójność i potencjalne błędy.
7. Konsola zarządzania musi umożliwiać graficzną prezentację i analizę struktury sieci chronionych. Mapa sieci musi być tworzona automatycznie na podstawie definicji obiektów.
8. Konsola zarządzania musi umożliwiać centralą aktualizację oprogramowania zabezpieczeń (m.in. instalację poprawek i nowych wersji).
9. Konsola zarządzania musi umożliwiać obserwację w czasie rzeczywistym stanu zajętości pasma sieci.

V. System korelacji zdarzeń i raportowania

1. Korelacja zdarzeń i raportowanie musi być realizowane z poziomu dedykowanego, dostarczonego systemu bądź z poziomu posiadanego przez Zamawiającego rozwiązania Check Point SmartEvent.
2. System korelacji zdarzeń musi posiadać możliwość detekcji ataków/zagrożeń zgłoszonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń.
   a) system korelacji musi analizować zdarzenia ze wszystkich modułów bezpieczeństwa,
   b) zdarzenia muszą być wyświetlane w formie różnego rodzaju statystyk i wykresów, muszą one być interaktywne i umożliwiać szczegółową analizę problemu,
   c) w celu usprawnienia pracy administratorów narzędzie do korelacji musi zawierać system zarządzania i obsługi incydentów bezpieczeństwa.
3. W ramach systemu musi zostać zapewniony system raportowania, który będzie umożliwiał generowanie predefiniowanych przez producenta raportów jak również tworzenie własnych .
   a) raporty muszą być generowanie cyklicznie lub na żądanie administratora,
   b) muszą być obsługiwane co najmniej następujące formaty: html , pdf,
   c) wygenerowany raport system powinien wysłać e-mailem do wskazanej listy osób.

Wymagania dodatkowe dotyczące urządzeń do transmisji danych cyfrowych

VI. Rozbudowa urządzenia

1. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego posiadające budowę modularną zapewniającą co najmniej trzy sloty pozwalające na ich wyposażenie w moduły co najmniej:
    a) 8-portowe 10/100/1000BASE-T RJ45,
    b) 4-portowe 1GE SFP,
    c) 4-portowe 10GE SFP+,
    d) 2-portowe 40GE QSFP+.

VII. URL filtering oraz Identyfikacja użytkownika

1. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego które posiada bazę znanych aplikacji większą niż 7000 pozycji oraz wspiera rozpoznawanie minimum 260.000 widgetów WEB 2.0.
2. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego które do automatycznego wykrywania i klasyfikowania aplikacji korzysta z lokalnego cache w celem optymalizacji tego mechanizmu.
3. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego które do filtrowania URL pozwala na kategoryzację względem ryzyka danego adresu.
4. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego które wspiera obsługę nagłówków pozwalających na identyfikację użytkownika np. X-forwarded.

VIII. Zaawansowane funkcjonalności eliminacji ataków zero-day

1. Urządzenie pełniące funkcję bezsygnaturowego wykrywania ataków zero-day poprzez analizę plików w wydzielonym środowisku wirtualnym które poza modułem umożliwiającym analizę podejrzanych plików w wydzielonym środowisku emulacyjnym, realizuje funkcję dostarczania bezpiecznych plików poprzez usunięcie z nich zawartości aktywnej.
2. Administrator musi mieć możliwość utworzenia listy adresatów oraz nadawców poczty e-mail, którzy mają być wykluczeni z inspekcji plików.

IX. Zaawansowane funkcjonalności administrowania

1. Urządzenie do korelacji zdarzeń i raportowania wyposażone w mechanizm który umożliwia administratorowi tworzenie własnych reguł korelacji.
2. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego którego system zarządzania:

2.1 dokonuje weryfikacja poprawności konfiguracji przez jej zainstalowaniem,

2.2 umożliwia wersjonowanie konfiguracji i pozwala na pracę na kilku (minimum 5) zapisanych konfiguracjach,

2.3 zmiany w konfiguracji reguł bezpieczeństwa przeprowadza w trybie off-line oraz umożliwia wdrażanie spójnej polityki bezpieczeństwa na wszystkich posiadanych i obsługiwanych urządzeniach jednocześnie,

2.4 ma możliwość automatycznego wycofania zmian w trakcie wdrażania spójnej polityki bezpieczeństwa jeśli na jednym z urządzeń nowa polityka nie zostanie poprawnie zainstalowana,

3. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego którego system zarządzania umiejscowiony jest poza zamawianymi urządzeniami (np. na dedykowanej maszynie wirtualnej)
4. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego którego system zarządzania posługuje się bazę obiektów dla stosu IPv4 oraz IPv6 charakteryzującą się tym, że dla danego obiektu możemy przypisać jednocześnie adres IPv4 oraz IPv6
5. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego które posiada wbudowane narządzie diagnostyczne tcpdump dostępne z poziomu konsoli CLI zamawianych urządzeń.

X. Integracja z posiadanymi przez zamawiającego systemami zarządzania firmy Check Point:

1. Urządzenie pełniące funkcję bezsygnaturowego wykrywania ataków zero-day poprzez analizę plików w wydzielonym środowisku wirtualnym którego zarządzanie politykami bezpieczeństwa oraz konfiguracja urządzenia jest realizowane z poziomu posiadanego przez zamawiającego rozwiązania Check Point Security Management Server R77.30
2. Urządzenie pełniące funkcję bezsygnaturowego wykrywania ataków zero-day poprzez analizę plików w wydzielonym środowisku wirtualnym które korelację zdarzeń i raportowanie realizuje z poziomu posiadanego przez Zamawiającego rozwiązania Check Point SmartEvent
3. Urządzenie wyposażone w system zarządzania konfiguracją oraz politykami bezpieczeństwa który integruje się w pełni z posiadanym przez zamawiającego rozwiązaniem Check Point Security Management Server R77.30
4. Urządzenia dające możliwość wykorzystania posiadanych przez zamawiającego licencji do uruchomienia funkcjonalności opisanych w OPZ