|  |
| --- |
| **MINIMALNE WYMAGANIA** |
| **System ochrony poczty (1 sztuka)** |  |
| Wymagania ogólne | System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:1. Tryb Gateway.2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej). |
| Parametry fizyczne systemu antyspamowego | 1. System musi być wyposażony w interfejsy:4 porty Gigabit Ethernet RJ-45.2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB .3. System musi posiadać wbudowany port konsoli szeregowej.4. Zasilanie z sieci 240V/50Hz. |
| Ogólne funkcje systemu ochrony poczty | Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:1. Wsparcie dla co najmniej 20 domen pocztowych.2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 28 tys wiadomości/godzinę.3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika. |
| Kontrola antywirusowa i ochrona przed malware | W tym zakresie dostarczony system ochrony poczty musi zapewniać:1. Skanowanie antywirusowe wiadomości SMTP.2. Kwarantannę dla zainfekowanych plików.3. Skanowanie załączników skompresowanych. 4. Definiowanie komunikatów powiadomień w języku polskim.5. Blokowanie załączników w oparciu o typ pliku.6. Możliwość zdefiniowania nie mniej niż 50 polityk kontroli antywirusowej.7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.9. Ochronę typu wirus outbrake. |
| Kontrola antyspamowa | System musi zapewniać poniższe funkcje i metody filtrowania spamu:1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.3. Szczegółowa kontrola nagłówka wiadomości. 4. Analiza Heurystyczna.5. Współpraca z zewnętrznymi serwerami RBL, SURBL.6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF. 9. Kontrola w oparciu o Greylisting oraz SPF.10. Filtrowanie treści wiadomości i załączników.11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.12. Możliwość zdefiniowania nie mniej niż 50 polityk kontroli antyspamowej.13. Ochrona typu outbrake.14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking). 15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. |
| Ochrona przed atakami na usługę poczty | System musi zapewniać poniższe funkcje i metody filtrowania:1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. 3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).5. Weryfikacja poprawności adresu e-mail nadawcy. |
| Funkcje logowania i raportowania | W tym zakresie dostarczony system ochrony poczty musi zapewniać:1. Logowanie do zewnętrznego serwera SYSLOG.2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.5. Możliwość analizy przebiegu sesji SMTP.6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu. 8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu. |
| Funkcje pracy w trybie wysokiej dostępności (HA) | System ochrony poczty musi zapewniać poniższe funkcje:1. Konfigurację HA w każdym z trybów: gateway, transparent.2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.4. Monitorowanie stanu pracy klastra. |
| Aktualizacje sygnatur, dostęp do bazy spamu | W tym zakresie dostarczony system ochrony poczty musi zapewniać:1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę. |
| Zarządzanie | System ochrony poczty musi zapewniać poniższe funkcje:1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.3. Powinna istnieć możliwość zdefiniowania lokalnych kont administracyjnych. |
| Certyfikaty | Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified. |
| Serwisy i licencje | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake na okres min. 12 miesięcy. |
| Gwarancja oraz wsparcie | System musi być objęty serwisem gwarancyjnym producenta przez okres min. 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| **Urządzenie typu firewall UTM (1 sztuka)** |  |
| Wymagania Ogólne | System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.System wspiera protokoły IPv4 oraz IPv6 w zakresie:• Firewall.• Ochrony w warstwie aplikacji.• Protokołów routingu dynamicznego. |
| Redundancja, monitoring i wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.3. Monitoring stanu realizowanych połączeń VPN.4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| Interfejsy, Dysk, Zasilanie | 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 8 portami Gigabit Ethernet RJ-45.2 gniazdami SFP 1 Gbps.2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.4. System jest wyposażony w zasilanie AC. |
| Parametry wydajnościowe | 1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.2. Przepustowość Stateful Firewall: nie mniej niż 6,5 Gbps dla pakietów 512 B.3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps. |
| Funkcje Systemu Bezpieczeństwa | W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.2. Kontrola Aplikacji.3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.4. Ochrona przed malware.5. Ochrona przed atakami - Intrusion Prevention System.6. Kontrola stron WWW.7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.8. Zarządzanie pasmem (QoS, Traffic shaping).9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.11. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |
| Polityki, Firewall | 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:• Translację jeden do jeden oraz jeden do wielu.• Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.• Amazon Web Services (AWS).• Microsoft Azure.• Cisco ACI.• Google Cloud Platform (GCP).• OpenStack.• VMware NSX.• Kubernetes. |
| Połączenia VPN | 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:• Wsparcie dla IKE v1 oraz v2.• Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).• Obsługa protokołu Diffie-Hellman grup 19, 20.• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.• Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.• Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.• Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.• Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.• Mechanizm „Split tunneling” dla połączeń Client-to-Site.2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.• Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |
| Routing i obsługa łączy WAN | W zakresie routingu rozwiązanie zapewnia obsługę:1. Routingu statycznego.2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.6. BFD (Bidirectional Forwarding Detection).7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| Funkcje SD-WAN | 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| Zarządzanie pasmem | 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.2. System daje możliwość określania pasma dla poszczególnych aplikacji.3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |
| Ochrona przed malware | 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| Ochrona przed atakami | 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |
| Kontrola WWW | 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| Logowanie | 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.4. Możliwość włączenia logowania per reguła w polityce firewall.5. System zapewnia możliwość logowania do serwera SYSLOG.6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| Certyfikaty | Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:ICSA lub EAL4 dla funkcji Firewall. |
| Serwisy i licencje | Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy. |
| Gwarancja oraz wsparcie | System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |