**AE/ZP-27-10/22 ZAŁĄCZNIK NR 3**

|  |  |
| --- | --- |
|  **LP** | **OPIS PARAMETRÓW URZĄDZENIA UTM** |
| **Obsługa sieci** |
|  | Urządzenie posiada wsparcie dla protokołu IPv4 oraz IPv6 na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. |
| **Firewall** |
|  | Urządzenie wyposażone w Firewall klasy Stateful Inspection. |
|  | Urządzenie obsługuje translacje adresów NAT n:1, NAT 1:1 oraz PAT  |
|  | Urządzenie ma możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). |
|  | Interface (GUI) do konfiguracji firewall umożliwia tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. |
|  | Administrator ma możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. |
|  | Rozwiązanie umożliwia między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. |
|  | Administrator ma możliwość zdefiniowania co najmniej 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. |
|  | Edytor reguł firewall posiada wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). |
|  | Firewall umożliwia uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows. |
| **IPS (Intrusion Prevention System - systemy wykrywania i zapobiegania włamaniom)** |
|  | System detekcji i prewencji włamań (IPS) jest zaimplementowany w jądrze systemu i wykrywa włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. |
|  | Moduł IPS.  |
|  | Moduł IPS zabezpiecza przed co najmniej 10 000 ataków i zagrożeń. |
|  | Administrator ma możliwość tworzenia własnych sygnatur dla systemu IPS |
|  | Moduł IPS nie tylko wykrywa, ale również usuwa szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej. |
|  | Urządzenie umożliwia inspekcję ruchu tunelowanego wewnątrz protokołu SSL w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. |
|  | Administrator urządzenia ma możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. |
|  | Urządzenie ma możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. |
| KSZTAŁTOWANIE PASMA (Traffic Shapping) |
|  | Urządzenie ma możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. |
|  | Ograniczenie pasma lub priorytetyzacja jest określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. |
|  | Rozwiązanie umożliwia tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). |
|  | Urządzenie umożliwia kształtowanie pasma na podstawie aplikacji generującej ruch. |
| OCHRONA ANTYWIRUSOWA |
|  | Rozwiązanie zezwala na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). |
|  | Jeden z dwóch skanerów antywirusowych dostarczany jest w ramach podstawowej licencji. |
|  | Administrator ma możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. |
|  | Administrator ma możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia. |
| OCHRONA ANTYSPAM |
|  | Producent udostępnia mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). |
|  | Ochrona antyspam działa w oparciu o:- Białe i czarne listy,- DNS RBL,- heurystyczny skaner |
|  | W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. |
|  | Wpis w nagłówku wiadomości zaklasyfikowanej jako spam jest w formacie zgodnym z formatem programu Spamassassin. |
| WIRTUALNE SIECI PRYWANTE (VPN) |
|  | Urządzenie posiada wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). |
|  | Odpowiednio kanały VPN można budować w oparciu o:- PPTP VPN,- IPSec VPN,- SSL VPN. |
|  | SSL VPN musi działać w trybach Tunel i Portal. |
|  | W ramach funkcji SSL VPN dostarczony jest klient VPN współpracujący z oferowanym rozwiązaniem.Rozwiązanie jest także kompatybilne z oprogramowaniem Open VPN |
|  | Urządzenie posiada funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). |
|  | Urządzenie posiada wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. |
|  | Urządzenie umożliwia tworzenie tuneli w oparciu o technologię Route Based. |
| FILTR DOSTĘPU DO STRON WWW |
|  | Urządzenie posiada wbudowany filtr URL |
|  | Filtr URL działa w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. |
|  | Administrator ma możliwość dodawania własnych kategorii URL. |
|  | Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. |
|  | Moduł filtra URL, wspierany przez HTTP PROXY, jest zgodny z protokołem ICAP co najmniej w trybie REQUEST. |
|  | Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:- blokowanie dostępu do adresu URL,- zezwolenie na dostęp do adresu URL,- blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. |
|  | Administrator ma możliwość zdefiniowania 4 różnych stron z komunikatem o zablokowaniu strony. |
|  | Strona blokady umożliwia wykorzystanie zmiennych środowiskowych. |
|  | Filtrowanie URL uwzględnia także komunikację po protokole HTTPS. |
|  | Urządzenie pozwala na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. |
|  | Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. |
| UWIERZYTELNIANIE |
|  | Urządzenie zezwala na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:- lokalną bazę użytkowników (wewnętrzny LDAP),- zewnętrzną bazę użytkowników (zewnętrzny LDAP),- usługę katalogową. |
|  | Rozwiązanie pozwala na równoczesne użycie 5 różnych baz LDAP. |
|  | Rozwiązanie zezwala na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły:- SSL,- Radius,- Kerberos. |
|  | Urządzenie posiada dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej. |
|  | Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta. |
|  | Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny. |
| ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP) |
|  | Urządzenie posiada wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). |
|  | Mechanizm równoważenia obciążenia łącza internetowego działa w oparciu o następujące dwa mechanizmy:- równoważenie względem adresu źródłowego,- równoważenie względem połączenia. |
|  | Mechanizm równoważenia łącza uwzględnia wagi przypisywane osobno dla każdego z łączy do Internetu. |
|  | Urządzenie posiada mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. |
|  | Urządzenie posiada mechanizm statycznego trasowania pakietów. |
|  | Urządzenie posiada możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. |
|  | Urządzenie posiada możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.  |
|  | Rozwiązanie zapewnia obsługę routingu dynamicznego w oparciu o protokoły: RIPv2, OSPF oraz BGP. |
|  | Rozwiązanie wspiera technologię Link Aggregation. |
| POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA |
|  | Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. |
|  | Urządzenie pozwala na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. |
|  | Konfiguracja serwera DHCP jest niezależna dla protokołu IPv4 i IPv6. |
|  | Urządzenie posiada możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS. |
|  | Urządzenie jest wyposażone w klienta usługi SNMP w wersji 1,2 i 3. |
|  | Urządzenie posiada usługę DNS Proxy. |
|  | Urządzenie posiada wsparcie dla Spanning-tree protocol (RSTP/MSTP). |
| ADMINISTRACJA URZĄDZENIEM |
|  | Konfiguracja urządzenia jest przeprowadzana z wykorzystaniem polskiego interfejsu graficznego. |
|  | Interfejs konfiguracyjny dostępny poprzez przeglądarkę internetową a komunikacja jest zabezpieczona za pomocą protokołu https. |
|  | Komunikacja może odbywać się na porcie innym niż https (443 TCP). |
|  | Urządzenie jest zarządzana przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. |
|  | Rozwiązanie ma możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji jest szyfrowana. |
|  | Interfejs konfiguracyjny platformy centralnego zarządzania jest dostępny poprzez przeglądarkę internetową a komunikacja jest zabezpieczona za pomocą protokołu https. |
|  | Urządzenie ma możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów jest możliwe za pomocą transmisji szyfrowanej (TLS). |
|  | Rozwiązanie ma możliwość eksportowania logów za pomocą protokołu IPFIX. |
|  | Urządzenie pozwala na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. |
|  | Urządzenie pozwala na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. |
|  | Urządzenie posiada funkcjonalność anonimizacji logów. |
| RAPORTOWANIE |
|  | Urządzenie posiada wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. |
|  | System raportowania i przeglądania logów wbudowany w system nie wymaga dodatkowej licencji do swojego działania. |
|  | System raportowania posiada predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. |
|  | System raportujący umożliwia wygenerowanie minimum 25 różnych raportów. |
|  | System raportujący daje możliwość edycji konfiguracji z poziomu raportu. |
|  | W ramach podstawowej licencji jest możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. |
|  | Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy. |
| PARAMETRY SPRZĘTOWE |
|  | Urządzenie jest wyposażone w dysk SSD o pojemności co najmniej 240 GB. |
|  | Liczba portów Ethernet 10/100/1000Mbps – min. 12. |
|  | Urządzenie posiada funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. |
|  | Przepustowość Firewall – minimum 8 Gbps. |
|  | Przepustowość Firewall wraz z włączonym systemem IPS minimum 3,3 Gbps. |
|  | Przepustowość filtrowania Antywirusowego minimum 950 Mbps. |
|  | Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 1,3 Gbps. |
|  | Maksymalna liczba tuneli VPN IPSec - 500. |
|  | Maksymalna liczba tuneli typu Full SSL VPN - 100. |
|  | Obsługa min. VLAN 256. |
|  | Liczba równoczesnych sesji - 500 000 i nie mniej niż 25 000 nowych sesji/sekundę. |
|  | Urządzenie daje możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. |
|  | Urządzenie jest nielimitowane na użytkowników. |  |