| Nazwa wymagania | Opis wymagania |
|---|---|
| Integracja z SIEM | System będzie umożliwiał integrację z system SIEM poprzez wysyłanie logów do SIEM. W systemie Firewall możliwe będzie zdefiniowanie, które logi będą wysyłane. |
| Integracja z SOAR | System umożliwia integrację z SOAR w celu pobierania z Firewall informacji o konfiguracji/logów i wysyłania do Firewall informacji mających wpływ na obsługę ruchu |
| Integracja z AD, LDAP w zakresie tworzenia reguł | Rozwiązanie powinno integrować się z AD, LDAP w zakresie tworzenia reguł opartych o grupy użytkowników. |
| Integracja z MISP | System posiada możliwość integracji z MISP Open Source Threat Intelligence Platform |
| Integracja z usługą katalogową (Active Directory) | Integracja z Active Directory / AD LDS do wykorzystania w procesie uwierzytelnienia do systemu |
| Integracja z o365 | Integracja z Microsoft o365 w kontekście utrzymywania listy dynamicznych dostępów do zasobów o365 |
| Konta uprzywilejowane | Integracja z systemem zarządzania kontami/hasłami np. PIM/PAM Cyber Ark |
| Dostęp do zasobów | Definicja dostępu do zasobów bazując na rolach, przynależności do OU, podsieci/segmentów organizacyjnych |
| Dostęp do zasobów | Dostęp do zasobów bazując na reputacji hosta wewnętrznego |
| Dostęp do zasobów | Dostęp do zasobów bazując na tożsamości, |
| URL filtering | Możliwość budowania reguł firewall na podstawie nazw domenowych |
| Czasowy dostęp do zasobów | Rozwiązanie wspiera tworzenie czasowych reguł dostępowych wprowadzanych ręcznie lub pozyskiwanych z kalendarzy użytkowników |

| | |
|---|---|
| URI filtering | tworzenie reguł na podstawie URI |
| FQDN filtering | tworzenie reguł na podstawie FQDN |
| Threat Inteligence | System zapewnia mechanizmy i dostęp do danych w celu identyfikacji i zapobiegania cyberzagrożeniom zidentyfikowanym przez Producenta sprzętu jako niebezpieczne. |
| Logowanie audytowe | Rozwiązanie powinno rejestrować logi audytowe (tworzyć dzienniki zdarzeń). Pojedynczy rekord logu audytowego powinien posiadać wystarczające informacje tj. typ zdarzenia, kiedy , gdzie nastąpiło, kto lub co spowodowało dane zdarzenie, |
| Logowanie połączeń | System umożliwia logowanie połączeń sieciowych, posiada możliwość granularnego definiowania logowania |
| IPS/IDS | System posiada funkcjonalność IPS/IDS |
| Blacklist, Whitelist | System powinien umożliwiać tworzenie Blacklist oraz Whitelist bazujących na serwerach reputacji, na FQDN, IP, URI |
| Deszyfracja ruchu | Deszyfracja ruchu w trybie:<br>- MitM<br>- terminacji SSL |
| Ochrona DoS/DDoS | Ochrona wewnętrznych zasobów przed atakiem DoS/DDoS w warstwie aplikacyjnej |
| SSL/TLS | Obsługa protokołów SSL/TLS, |
| Agent na hostach | Rozwiązanie posiada możliwość instalacji agenta na hostach i pozyskiwanie informacji na bazie których realizowany jest dostęp do zasobów. |
| ICAP | System posiada obsługę protokołu ICAP |
| Dodatkowe funkcjonalności | Funkcjonalność antyvirus,antymalware,antyspyware |
| Firewall | Firewall w funkcji routingu. |

| | |
|---|---|
| | Firewall- stanowy, dokonuje działania w oparciu o wiedzę o aktywnych sesjach. |
| Firewall - Warstwa 4 | Firewall dokonuje inspekcji ruchu w oparciu o protokoły warstwy transportowej modelu OSI |
| Routing dynamiczny | Urządzenie wspiera dynamiczny protokół routingu OSPF i BGP. |
| Budowanie polityk dostępowych | System powinien posiadać możliwość ręcznego budowania reguł , w tym definiujących działania niepożądane |
| Reakcja na zdarzenia | System umożliwi zdefiniowanie wymienionej reakcji na zdarzenia<br>Zezwól/Blokuj/Poinformuj/Zapisz do logu |
| Tworzenie polis bazujących na dodatkowych cechach | Firewall umożliwi konfigurowanie anulowania sesji bezczynnych przez określony czas |
| Licznik ilości sesji dopasowanych do reguły | System przedstawia informację o ilości sesji dopasowanych do danej reguły, bez konieczności włączania logowania reguł, |
| Sposoby powiadamiania | System umożliwi powiadamianie za pomocą wymienionego mechanizmu:<br>email<br>zapisanie do logu<br>wysłanie do serwera syslog<br>wysłanie do serwera SIEM |
| Możliwość samodzielnego zdefiniowania formatu wysyłanej informacji w przypadku: | System umożliwi zdefiniowanie formatu wysyłanej jako powiadomienie wiadomości email/syslog |
| Przechwytywanie fragmentu ruchu | Możliwość przechwytywania dowolnego ruchu przechodzącego przez FW do pliku PCAP. |
| NetFlow | Obsługa protokołu NetFlow |

| | |
|---|---|
| Logowanie zdarzeń | System zapisuje w logach wszelkie zdarzenia, które naruszają zdefiniowane reguły i polityki. Logi stanowią kompletny zapis przebiegu zdarzeń. |
| Składowanie logów | Sposób składowania logów nie wpływa negatywnie na prace urządzenia |
| Zakres informacyjny i składowanie logu | Logi powinny zawierać informacje:<br>• adres źródłowy i docelowy;<br>• protokół / port L4<br>• data zdarzenia (dzień, miesiąc, rok, godzina, sekunda, milisekunda),<br>• szczegóły naruszenia, (jaka reguła, polityka),<br>• opcjonalnie: stopień naruszenia (waga) - jeżeli zostało zdefiniowane. |
| Kryteria filtrowania zdarzeń: | naruszona polityka<br>adres źródłowy, docelowy<br>protokół / port<br>czas wystąpienia<br>waga zdarzenia (opcjonalnie) |
| Raportowanie | System powinien umożliwiać generowanie raportów z zalogowanych zdarzeń |
| Predefiniowane raporty | System powinien posiadać listę predefiniowanych raportów. |
| Budowanie własnych raportów | System umożliwi budowanie własnych raportów. |
| Identyfikacja nieużywanych polis | System umożliwia detekcję nieużywanych polis oraz możliwość ich wyeksportowania do pliku w postaci raportu. |

| | |
|---|---|
| Zakres informacyjny raportu | Raport powinien zawierać:<br>• adres źródłowy i docelowy;<br>• protokół / port L4<br>• data zdarzenia (dzień, miesiąc, rok, godzina, sekunda, milisekunda),<br>• szczegóły naruszenia, (jaka reguła, polityka),<br>• opcjonalnie: stopień naruszenia (waga) - jeżeli zostało zdefiniowane. |
| Retencja logów | Możliwość ustawień przechowywania i backupowania logów, minimum 7 dni online |
| Eksport zdarzeń | System powinien umożliwiać możliwość wyeksportowania wybranych alertów. (eksport odfiltrowanych alertów) |
| Scentralizowana konsola zarządzająca | System powinien zapewnić scentralizowane zarządzanie jego komponentami. |
| Szyfrowanie komunikacji | System powinien umożliwiać konfigurację protokołu szyfrowania w komunikacji pomiędzy urządzeniami systemu a konsolą administratora |
| 2FA | System umożliwia opcję 2 czynnikowego uwierzytelnienia |
| Ograniczenie dostępu do konsoli zarządczej | System umożliwia ograniczanie dostępu do konsoli zarządczej |
| Liczba operatorów jednocześnie pracujących | System powinien zapewnić bezawaryjną, komfortową pracę 10 osób jednocześnie. |
| Możliwość przywrócenia poprzedniej wersji polityki | System powinien zapewnić możliwość przywrócenia poprzedniej wersji polityki |
| Zatwierdzanie poprawek | System będzie posiadał mechanizm zatwierdzania poprawek systemowych przez administratora. |
| Zarządzanie wgrywaniem aktualizacji lub polityk | Syetem będzie posiadał mozliwość planowania wgrywania aktualizacji lub polityk. |

| | |
|---|---|
| Archiwizacja raportów i plików na zasoby zewnętrzne | Rozwiązanie powinno posiadać możliwość wysyłania/kopiowania raportów i plików na zasoby zewnętrzne |
| Traffic shaping | Możliwość zastosowania mechanizmu traffic shaping. |
| Monitorowanie dostępności i pojemności | System musi mieć możliwość podłączenia czujek monitorujących (Obsługa protokołu SNMP w wersjach SNMP 2c i 3) |
| Interfejs API | System umożliwia integrację za pomocą interfejsu API zgodnego z architekturą REST, i możliwość automatyzacji i orchestracji |
| Protokół IPv6 | Wsparcie dla protokołu IPv6 w modelu dual stack (równoczesne działanie protokołów IPv4 i IPv6) |
| VPN | Funkcjonalność IPSec VPN i SSL VPN, możliwość uwierzytelnienia dwuskładnikowego i za pomocą certyfikatów, minimum 100 sesji |
| Radius/Tacacs | System posiada możliwość wykorzystania protokołów Radius /Tacacs w procesie AAA |
| Konfiguracja | Możliwość konfiguracji parametrów pracy narzędzia przez administratora w bez konieczności restartu narzędzia |
| Interfejsy połączeniowe (per urządzenie) | System posiada interfejsy elektryczne o przepustowości 1 Gb/s do podłączenia management/konsola w ilości 12 szt.<br>System posiada możliwość zastosowania interfejsów optycznych o przepustowości minimum 10 Gb/s - minimalna ilośc interfejsów 2 szt. |
| Minimalna przepustowość urządzenia | Sumarycznie jedno urządzenie dla ruchu TCP/UDP zapewnia przepustowość 10 Gb/s mierzonej dla warstwy sieciowej. |

| | |
|---|---|
| Wydaność systemu | W zakresie Firewall'a obsługa nie mniej niż 1,2 mln jednoczesnych sesji oraz 50.000 nowych połączeń na sekundę<br>Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps.<br>Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 10 Gbps.<br>Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control- minimum 17 Gbps. |
| Dostępność systemu na poziomie 99,9% w ciągu miesiąca | Dostępność systemu na poziomie 99,9% w ciągu miesiąca |
| Zasilanie | Pojedyńczy system powinien posiadać dwa zasilacze |