| Parametr | Charakterystyka |
|---|---|
| Elementy systemu bezpieczeństwa | • Urządzenie musi mieć możliwość jednoczesnej pracy w trybie Layer 3 (routing), transparentnym (most ) i Layer 2 (port mirroring) bez konieczności wirtualizacji sprzętu<br>• System pełniący funkcję zapory musi mieć co najmniej 8 interfejsów Ethernet 10/100/1000<br>• Możliwość stworzenia minimum 128 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q.<br>• W zakresie Firewall, obsługa nie mniej niż 1 100 000 jednoczesnych połączeń i 110 000 nowych połączeń na sekundę.<br>• System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o minimalnej pojemności 8 GB do celów logowania i raportowania.<br>• Możliwość rozszerzenia pamięci do 2 TB poprzez dodatkowy dysk SSD bez otwierania obudowy urządzenia<br>• Musi posiadać min. 1 port USB 3.0 z przodu urządzenia<br>• System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu.<br>• System musi mieć możliwość włączenia min 1 systemu wirtualnego bez dodatkowej licencji i możliwości rozszerzenia do min. 4 poprzez dodatkową licencję w przyszłości<br>• Systemy wirtualne muszą obsługiwać QOS |
| Funkcjonalności | • Kontrola dostępu — zapora sieciowa Stateful Inspection<br>• Ochrona przed wirusami - komercyjny antywirus [AV]<br>• Poufność danych - IPSec VPN i SSL VPN<br>• Kontrola witryn sieci Web — filtr URL<br>• Kontrola zawartości poczty – antyspam (dla protokołów SMTP, POP3)<br>• Kontrola przepustowości i ruchu (QoS i kształtowanie ruchu) z alokacją Tunnel w oparciu o strefę bezpieczeństwa, interfejs, adres, użytkownika/grupę użytkowników, serwera/ grupę serwerów, aplikację/grupę aplikacji, TOS, VLAN<br>• Kontrola aplikacji i rozpoznawanie ruchu P2P oraz ograniczanie nowych połączeń i jednoczesnych sesji<br>• Reputacja IP<br>• Cloud Sandbox |

| | |
|---|---|
| Wydajność | • Analiza ruchu szyfrowanego protokołem SSL<br>• Wydajność Firewall co najmniej 5 Gb/s<br>• Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym IPS i kontrolą aplikacji 2,5 Gb/s<br>• Wydajność ochrony przed atakami (IPS) minimum 4 Gb/s<br>• Wydajność AV nie mniej niż 3,5Gb/s |
| Funkcjonalności VPN | • Wydajność IPSec VPN, nie mniej niż 2,5 Gb/s<br>• Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja<br>• Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem.<br>• Monitorowanie stanu tuneli VPN i utrzymywanie ich aktywności<br>• Praca w topologiach Hub and Spoke i Mesh<br>• Wspierane mechanizmy : IPSec NAT Traversal, DPD, Replay Detection, Xauth, DHCP over IPsec,<br>• Wsparcie grup DH (Diffie-Hellman) dla IKEv1: 1,2,5,19,20,21,24<br>• Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,19,20,21,24<br>• Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance)<br>• Obsługa PnPVPN (Plug and Play VPN) |
| Routing | • Rozwiązanie musi zapewniać: obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP, IS-IS<br>• Obsługa Policy Based Routing<br>• Funkcjonalność Virtual Wire |
| Translacja adresów NAT | • Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego.<br>• Obsługa NAT46, NAT64, DNS64<br>• Wsparcie dla STUN (Session Traversal Utilities for NAT) |
| Polityka bezpieczeństwa systemu | • Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje bezpieczeństwa, rejestrowanie zdarzeń i zarządzanie pasmem sieci (w tym gwarantowaną i maksymalną przepustowość, priorytety).<br>• Możliwość budowania min. 8000 polityk<br>• Musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego<br>• Musi być w stanie skonfigurować agregowane polityki |

| | |
|---|---|
| | • Musi być w stanie ograniczyć sesje na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu aplikacji (mysql, ms-sql, sqlnet, pobieranie P2P) |
| Wydzielenie stref bezpieczeństwa | • Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN<br>• Musi mieć możliwosc konfiguracji oddzielnych wirtualnych routerów<br>• Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników |
| Ochrona antywirusowa | • Silnik antywirusowy musi by ć oparty na przepływie tzw. flow-based<br>• Musi umożliwiać skanowanie protokołów HTTP, SMTP, POP3, IMAP, FTP / SFTP, SMB<br>• Możliwość ręcznego dodawania lub usuwania sygnatury MD5 do bazy danych AV<br>• Musi obsługiwać wykrywanie wirusów w plikach skompresowanych, takich jak RAR, ZIP, GZIP, BZIP2, TAR, a także wykrywać wielowarstwowe pliki skompresowane dla nie mniej niż 5 warstw dekompresji |
| Rownoważenie obciążenia | • Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łącza dla określonej nazwy domeny oraz monitorowanie stanu łącza poprzez aktywną metodę wykrywania<br>• Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted least-connection i weighted round-robin<br>• Kontrola stanu serwera, monitorowanie sesji i ochrona sesji |
| Ochrona IPS | • Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury.<br>• Baza danych wykrytych ataków musi zawierać co najmniej 11000 sygnatur. Dodatkowo musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i DDos.<br>• Funkcjonalność zapobiegania atakom SQL injection, XSS injection<br>• Możliwość budowania własnych niestandardowych reguł IPS |
| Obrona przed atakiem | • Ochrona przed nieprawidłowym działaniem protokołu<br>• Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment itp.<br>• Wsparcie IPv4 jak i IPv6 dla o chrony przed DNS query flood i DNS reply flood<br>• Biała listę docelowych adresów IP |

| | |
|---|---|
| Kontrola aplikacji | • Kontrola aplikacji musi być w stanie kontrolować ruch w oparciu o głęboką analizę pakietów, a nie tylko w oparciu o wartości portów TCP/UDP.<br>• Baza danych aplikacji zawierająca ponad 4600 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka |
| Filtr adresów URL | • Baza filtrów URL pogrupowana w co najmniej 60 kategorii tematycznych. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków.<br>• Możliwość zdefiniowania własnej bazy kategorii www.<br>• Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL.<br>• Kategoria takie jak hazard, malware, spam, botnety<br>• Obsługa Safe Search<br>• Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne<br>• Możliwość dostosowania strony ostrzeżenia użytkownika |
| Ochrona danych | • Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy<br>• Identyfikacja protokołu pliku, w tym HTTP、FTP、SMTP, POP3、IMAP<br>• Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS<br>• Filtrowanie plików przesyłanych przez SMB |
| Reputacja IP | • Identyfikacja i filtrowanie ruchu z ryzykownych adresów IP, takich jak hosty botnet, spamerzy, węzły Tor, podejrzane hosty i adresy IP atakujące metodą brute force<br>• Logowanie, odrzucanie pakietów lub blokowanie dla różnych rodzajów ryzykownego ruchu IP |
| Zapobieganie botnetom | • Wykrywanie intranetowych hostów botnetu, monitorując połączenia C&C i blokowanie dalszych zaawansowanych zagrożeń takich jak botnet i oprogramowanie ransomware<br>• Wsparcie DNS sinkhole<br>• Wsparcie wykrywania tunelowania DNS<br>• Wyrywanie i blokowanie DGA |
| Cloud Sandbox | • Złośliwe oprogramowanie emulowane w wirtualnym środowisku oparte na architekturze chmury w celu wykrywania nieznanych zagrożeń<br>• Obsługa protokołów, takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB |

| | |
|---|---|
| | • Obsługa typów plików : PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów<br>• Obsługa blokowania wyników wykrywania w celu szybkiego blokowania nieznanych zagrożeń. |
| Uwierzytelnianie użytkownika | • System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika poprzez:<br>– Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu<br>– Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP<br>– Hasła dynamiczne (RADIUS) oparte o zewnętrzne bazach danych<br>– Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA<br>• Musi umożliwiać budowę architektury uwierzytelniania pojedynczego logowania w środowisku Active Directory<br>• Wsparcie usług terminalowych<br>• Uwierzytelnianie użytkownika przez Web przed dotępem do internetu<br>• Obsługa dwuskładnikowego uwierzytelniania poprzez SMSy, certyfikaty i tokeny |
| Raportowanie i przeglądanie logów | • Wbudowany w system bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie |
| System logowania | • Wraz z systemem musi być zapewniony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy chmurowej, do której dostęp jest cały czas z dowolnego urządzenia oraz dedykowanej aplikacji mobilnej. |
| Certyfikaty | Rozwiązanie musi:<br>• posiadać certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSA Labs dla funkcji Firewall |
| Zarządzanie | • Elementy systemu muszą mieć możliwość zarządzania lokalnie (HTTPS, SSH) oraz współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja między systemami bezpieczeństwa a platformami zarządzania musi odbywać się za pomocą protokołów szyfrowanych.<br>• Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI bez instalowania oddzielnego oprogramowania, takiego jak dedykowana konsola |
| Gwarancja | Dostawa musi zawierać również:<br>• Minimalną 36-miesięczną gwarancję producenta na dostarczone elementy systemu |

| | |
|---|---|
| | • Licencje na wszystkie funkcje bezpieczeństwa urządzenia na okres minimum 36 miesięcy<br>• Wsparcie techniczne dystrybutora rozwiązań w języku polskim w trybie 8x5 |