**Załącznik nr 2 do SWZ**

**Oznaczenie postępowania: ZP 5/2023**

1. **Urządzenie NIPS (Network Intrusion Prevention System)**

|  |  |  |
| --- | --- | --- |
| Parametr  | Charakterystyka  | Oferowany parametr |
| Dane techniczne  | * Proponowane rozwiązanie powinno mieć maksymalną wysokość 1U.
* Proponowane rozwiązanie musi posiadać co najmniej dwa porty USB.
* Proponowane rozwiązanie musi posiadać co najmniej jeden port konsoli
* Proponowane rozwiązanie musi posiadać co najmniej jeden dedykowany port do zarządzania systemem
* Proponowane rozwiązanie musi posiadać co najmniej 8 stałych portów Gigabit Ethernet.
* Proponowane rozwiązanie musi posiadać co najmniej 8 stałych portów SFP.
* Proponowane rozwiązanie musi posiadać co najmniej 2 stałe porty SFP+.
* Proponowane rozwiązanie musi posiadać co najmniej 500GB przestrzeni dyskowej.
* Proponowane rozwiązanie musi obsługiwać przepustowość IPS 3 Gb/s
* Proponowane rozwiązanie musi obsługiwać jednoczesne sesje o długości 1.2 M
* Proponowane rozwiązanie musi obsługiwać min 40000 nowych sesji/sekundę w ruchu TCP.
* Opóźnienia (tzw. Latency) nie powinny przekraczać 300µs
* Funkcjonalności nie mogą być realizowane na rozwiązaniu NGFW

  |  |
| Usługi sieciowe | * Proponowane rozwiązanie musi być w stanie pracować jednocześnie w trybie warstwy 3 (routing), trybie online (most) i warstwie 2 (kopia ruchu) (bez konieczności wirtualizacji sprzętu)
 |  |
| Kontrola aplikacji | * Rozwiązanie powinno obsługiwać identyfikację IP hostów, ilość endpointów , czasu online, czasu offline.
* Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka.
* Rozwiązanie powinno rozpoznawać aplikacje IPv6.
* Rozwiązanie musi obsługiwać identyfikację aplikacji dla ruchu szyfrowanego SSL
* Rozwiązanie musi wspierać identyfikację aplikacji mobilnych na Androida i iOS.
* Rozwiązanie powinno obsługiwać wyświetlanie opisu, czynników ryzyka, zależności, typowych używanych portów i adresów URL dla dodatkowych odwołań i informacji dla każdej aplikacji w interfejsie WebUI.
* Rozwiązanie musi obsługiwać blokowanie, ponowne uruchamianie sesji, monitorowanie i kształtowanie ruchu dla aplikacji.
* Rozwiązanie musi być w stanie identyfikować i kontrolować aplikacje w chmurze
 |   |
| Ochrona przed zagrożeniami | * Rozwiązanie musi obsługiwać ponad 15000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, automatyczne wstawianie lub wyodrębnianie sygnatur oraz zintegrowaną encyklopedię zagrożeń.
* Rozwiązanie musi obsługiwać zapobieganie włamaniom dla ruchu szyfrowanego SSL.
* Rozwiązanie musi obsługiwać ochronę środowiska IPV6.
* Rozwiązanie musi obsługiwać ochronę przed sql injection, CC i atakom XSS.
* Rozwiązanie musi obsługiwać sprawdzanie linków zewnętrznych.
* Rozwiązanie powinno obsługiwać ochronę przed atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, metodami przyjaznymi dla robotów. Wspierane powinny być 4 metody uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA
* Rozwiązanie powinno obsługiwać wykrywanie anomalii protokołu.
* Rozwiązanie musi obsługiwać następujące akcje IPS: monitorowanie, blokowanie, resetowanie (adres IP atakujących lub IP ofiary, interfejs wejściowy) z czasem wygaśnięcia
* Rozwiązanie musi obsługiwać opcję logowania pakietów.
* Rozwiązanie musi obsługiwać profil zabezpieczeń IPS na podstawie ważności, obiektu docelowego, systemu operacyjnego, aplikacji lub protokołu.
* Rozwiązanie musi obsługiwać zapobieganie włamaniom dla protokołów HTTP, SMTP, IMAP. POP3, VOIP, NETBIOS itp.
* Rozwiązanie musi być wspierać weryfikację protokołów http typu Get, Head, Put, Post.
* Rozwiązanie musi obsługiwać wyłączenie IP z określonych sygnatur IPS.
* Rozwiązanie musi obsługiwać tryb działania sniffera IDS.
* Rozwiązanie musi obsługiwać predefiniowaną konfigurację profili IPS.
* Rozwiązanie musi obsługiwać tworzenie zdefiniowanych przez użytkownika sygnatur IPS.
* Proponowane rozwiązanie musi obsługiwać wykrywanie reputacji IP i blokowanie adresów IP serwera botnetów za pomocą globalnej bazy danych reputacji IP.
* Proponowane rozwiązanie powinno wspierać szczegółowy opis predefiniowanych profili IPS.
* Rozwiązanie musi obsługiwać rejestrację zagrożeń IPv6: obsługa przechwytywania i pobierania pakietów IPv6
* Szczegóły zagrożeń muszą obsługiwać identyfikator URI i dekodowanie danych ataków
* Obsługa wykrywania anomalii protokołów HTTP/DNS/FTP/MSRPC/POP3/SMTP/SUNRPC i Telnet
* Obsługa inspekcji Reverse Shell
* Blokowanie plików po rozszerzeniu dla minimum 100 typów plików
* Rozwiązanie musi wykrywać i blokować wrażliwe zrefowanych informacje w przesyłanych plikach dla minimum doc/docx, xls/xlsx, ppt/pptx, txt w protokołach HTTP, FTP, SMTP, POP3, IMAP, SMB
* Ochrona i wykrywanie skanowania protokołow IP oraz UDP
* Rozwiązanie musi mieć możliwość inspekcji payloudu w ramkach MPLS
* System musi mapować wykryte zagrożenia na taktyki MITRE ATT&CK
 |  |
| Antywirus | * Rozwiązanie musi obsługiwać ponad 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur.
* Rozwiązanie musi obsługiwać antywirus oparty na przepływie dla protokołów HTTP, SMTP, POP3, IMAP, FTP/SFTP, SMB
* Rozwiązanie powinno obsługiwać wykrywanie wirusów dla skompresowanych plików, takich jak RAR, ZIP, GZIP, BZIP2, TAR; obsługa wielowarstwowego wykrywania skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji
* Rozwiązanie musi obsługiwać akcje niestandardowe dla zaszyfrowanych plików skompresowanych.
* Rozwiązanie musi obsługiwać co najmniej 3 działania: usuwanie złośliwego kodu, resetowanie połączenia lub logowanie tylko po wykryciu wirusa lub złośliwej strony internetowej
* Rozwiązanie powinno obsługiwać ostrzeganie przed wirusami i złośliwymi stronami internetowymi, ostrzegać użytkownika, że witryna jest szkodliwą witryną lub że wykryto wirusa.
* Rozwiązanie musi obsługiwać funkcje AV w środowiskach IPV6.
 |  |
| Filtrowanie adresów URL | * Rozwiązanie musi obsługiwać dynamiczne filtrowanie sieci Web za pomocą chmurowej bazy danych kategoryzacji w czasie rzeczywistym: ponad 140 milionów adresów URL z co najmniej 64 kategoriami (z których nie mniej niż 8 jest związanych z bezpieczeństwem)
* Rozwiązanie musi obsługiwać ręcznie zdefiniowane filtrowanie sieci Web na podstawie adresu URL, zawartości sieci Web i nagłówka MIME
* Rozwiązanie musi obsługiwać następujące dodatkowe funkcje filtrowania.
* - Aplet Java, ActiveX lub filtr plików cookie.
* - Blokowanie postów HTTP
* - Rejestrowanie wyszukiwania słów kluczowych
* - Wykluczanie ze skanowania połączeń szyfrowanych w niektórych kategoriach dla prywatności.
* Rozwiązanie musi obsługiwać zastępowanie profilu filtrowania adresów URL, aby administrator mógł tymczasowo przypisać różne profile do użytkownika/grupy/adresu IP
* Rozwiązaniem powinno być umożliwienie dostosowania strony ostrzeżenia do filtrowania adresów URL.
 |  |
| Sandbox | * Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do chmury w celu analizy
* Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB
* Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR , SWF i Skryptów
* Rozwiązanie musi obsługiwać kierunek transferu plików i kontrolę rozmiaru pliku.
* Rozwiązanie musi zawierać kompletny raport analizy zachowania złośliwych plików
* Rozwiązanie powinno obsługiwać blokowanie zgodnie z wynikami wykrywania, aby szybko zablokować nieznane zagrożenie.
* Rozwiązanie musi obsługiwać udostępnianie globalnych informacji o zagrożeniach i blokować nieznane zagrożeni na całym świecie
 |  |
| Zapobieganie C&C Botnetom | * Rozwiązanie musi być w stanie skutecznie wykrywać boty intranetowe i zapobiegać dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównanie uzyskanych informacji z bazą adresów C&C
* Rozwiązanie musi obsługiwać regularne aktualizacje adresów serwerów botnetu.
* Rozwiązanie musi obsługiwać dwa typy bazy danych adresów C&C: bazę danych adresów IP (z wyłączeniem adresów IPv6) i bazę danych domen
* Rozwiązanie musi obsługiwać wykrywanie dla protokołów TCP, HTTP i DNS.
* Rozwiązanie musi obsługiwać umieszczanie adresów IP i domen na białej liście.
* Rozwiązanie musi obsługiwać funkcjonalność DNS Sinkhole i wykrywanie tunelowania DNS.
 |  |
| Monitoring | * Rozwiązanie musi posiadać pełne monitorowanie zagrożeń, w tym nazwę ataku, ważność, czasem, adresem, protokołem, zalecanym rozwiązaniem itp.
* Rozwiązanie musi obsługiwać usługę Threat Intelligence Pushing Service
* Rozwiązanie musi obsługiwać statystyki i analizy ruchu w czasie rzeczywistym.
* Rozwiązanie powinno obsługiwać monitorowanie stanu procesora, pamięci, temperatury, wentylatora, modułów zasilania itp.
 |  |
| Polityki bezpieczeństwa | * Proponowane rozwiązanie musi obsługiwać kontrolę dostępu do strefy (zone)、użytkownika 、 usługi, aplikacji, IPS, AV w jednej regule polityki.
* Proponowane rozwiązanie musi obsługiwać wstępnie zdefiniowane i niestandardowe obiekty
* Proponowane rozwiązanie musi obsługiwać weryfikację nadmiarowości polityki bezpieczeństwa oraz zliczanie trafień polityki przez interfejs WebUI
* Rozwiązanie musi obsługiwać import i eksport polityk
 |  |
| Administrowanie, logi i raportowanie | * Rozwiązanie musi być obsługiwane przez WebUI i interfejs wiersza poleceń (CLI)
* Rozwiązanie powinno obsługiwać zarządzanie dostępem przez HTTP/HTTPS, SSH, telnet, konsolę
* Rozwiązanie musi obsługiwać uwierzytelnianie dwuskładnikowe: nazwa użytkownika/hasło, plik certyfikatu HTTPS
* Rozwiązanie musi obsługiwać integrację systemu: SNMP, syslog.
* Rozwiązanie musi obsługiwać co najmniej 3 role administratora, w tym administratora, operatora i audytora
* Rozwiązanie musi być w stanie chronić system przed atakami brute force na nazwę użytkownika i hasło
* Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów.
* Rozwiązanie musi obsługiwać serwery Radius, AD i LDAP.
* Rozwiązanie musi obsługiwać szybkie wdrażanie poprzez automatyczne instalowanie z USB, uruchamianie skryptów lokalnych i zdalnych.
* Rozwiązanie musi obsługiwać dynamiczny dashboard w czasie rzeczywistym i szczegółowe widżety monitorowania
* Urządzenie musi obsługiwać zarządzanie urządzeniami pamięci masowej: dostosowywanie i alarmowanie progu przestrzeni dyskowej, nakładanie starych danych, zatrzymywanie nagrywania ruchu.
* Urządzenie musi obsługiwać szczegółowe logi ruchu: przekazane, sesje naruszone, ruch lokalny, nieprawidłowe pakiety
* Urządzenie musi obsługiwać pełne logi zdarzeń: audyty aktywności systemu i zarządzania, routing i sieć, VPN, uwierzytelnianie użytkowników, zdarzenia związane z Wi-Fi
* Urządzenie musi obsługiwać opcję rozpoznawania nazw portów usług i adresów IP.
* Rozwiązanie musi mieć możliwość dodania adresów IP lub MAC hostów do czarnej listy, aby zablokować dostęp przez określony czas.
* Rozwiązanie powinno obsługiwać blokowanie konta po kilku niepowodzeniach logowania.
* Rozwiązanie musi obsługiwać konfigurację zadań przechwytywania pakietów z wieloma warunkami przechwytywania pakietów w tym samym czasie oraz ich export
* Rozwiązanie musi obsługiwać standardowy SYSLOG i logowanie w formacie binarnym; rozproszone binarne przechowywanie logów na wielu serwerach logów
* Rozwiązanie powinno obsługiwać logowanie w pamięci lokalnej i/lub serwerach syslog.
* Rozwiązanie musi obsługiwać rejestrowanie zmiany w politykach
* Rozwiązanie musi obsługiwać logowanie zaufane przy użyciu opcji TCP (RFC 3195)
* Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika.
* Rozwiązanie musi obsługiwać zaplanowany raport.
* Raport można wyeksportować w formacie PDF/HTML/WORD za pośrednictwem email lub FTP.
* Rozwiązanie musi umożliwić podgląd raportów w formacie HTML i PDF.
 |  |
| Wysoka dostępność | * Rozwiązanie musi obsługiwać tryby Active/Active i Active/Passive
* Rozwiązanie musi obsługiwać następujące opcje wdrażania HA:
* - HA z agregacją linków
* - Full mesh HA
* - Geograficznie rozproszony HA
* Rozwiązanie musi obsługiwać funkcję bypass sprzętowych interfejsów i dedykowany interfejs HA
 |  |
| QoS | * Rozwiązanie musi obsługiwać maksymalną lub gwarantowaną kontrolę przepustowości dla adresów IP lub użytkowników.
* Rozwiązanie powinno obsługiwać tunelowanie w oparciu o domenę zabezpieczeń, interfejs, adres, pulę użytkowników/użytkowników, pulę serwer/serwer, pulę aplikacji/aplikacji, TOS, sieci VLAN.
* Rozwiązanie musi obsługiwać przepustowość przydzieloną w zakresie - czas, priorytet lub tę samą współdzieloną przepustowość
* Rozwiązanie musi obsługiwać typ usługi (TOS) i zróżnicowane usługi (DiffServ)
* Rozwiązanie musi obsługiwać tworzenie zaplanowanych polityk QoS.
* Rozwiązanie musi obsługiwać elastyczną, priorytetową alokację pozostałej niewykorzystanej przepustowości.
* Rozwiązanie musi obsługiwać dwa poziomy konfiguracji ruchu, które umożliwiają konfigurację ruchu w różnych wymiarach, takich jak użytkownicy i aplikacje. Rozwiązanie musi obsługiwać co najmniej cztery tunele na poziom, co zapewnia hierarchię kontroli ruchu.
* Rozwiązanie musi obsługiwać alokację przepustowości na podstawie kategorii adresu URL
* Rozwiązanie musi obsługiwać adresy IPv6 w funkcji QoS.
 |  |
| Ochrona przed spamem | * Rozwiązanie musi obsługiwać klasyfikację spamu w czasie rzeczywistym i zapobieganie mu.
* Rozwiązanie musi obsługiwać ochronę niezależnie od języka, formatu lub zawartości wiadomości.
* Rozwiązanie musi obsługiwać protokoły poczty e-mail SMTP i POP3.
* Rozwiązanie musi obsługiwać wykrywanie zarówno ruchu przychodzącego, jak i wychodzącego.
* Rozwiązanie musi obsługiwać białe listy, aby umożliwić wysyłanie wiadomości e-mail z zaufanych domen.
* Rozwiązanie musi obsługiwać listę obejść opartą na nadawcy i niestandardowe reguły spamu.
* Rozwiązanie musi mieć możliwość konfiguracji czarnych i białych list dla modułu Anti-Spam
 |  |
| Reputacja IP | * Obsługa filtrowania ruchu z adresów IP o niskiej reputacji, w tym botnetów, spamu, węzłów Tora, skompromitowanych, Brute-force itp.
* Obsługa rejestrowania, usuwania lub blokowania pakietów, jeśli złośliwy ruch dotrze do listy reputacji IP.
* Obsługa uaktualniania bazy danych przez zainstalowanie licencji IP Reputation.
* Obsługa filtrowania adresów IP botów.
 |  |
| Gwarancja i dostawa | * Dostawa musi zawierać również:
* 36-miesięczną gwarancję producenta na dostarczone elementy systemu
* Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 36 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)
* Wsparcie techniczne dystrybutora rozwiązań w języku polskim
 |  |

1. **System NDR (Network Detection and Response)**

|  |  |  |
| --- | --- | --- |
| Parametr  | Charakterystyka  | Oferowany parametr |
| Dane techniczne | * Wysokość 1U do montażu w szafie rack.
* Posiadać co najmniej dwa porty USB
* Urządzenie musi posiadać dedykowany port do zarządzania
* Urządzenie musi posiadać minimum interfejsów: 2x SFP+, 8x SFP, 8x GE
* Musi obsługiwać co najmniej 1T przestrzeni dyskowej.
* Minimum 1 Gb/s przepustowości wykrywania naruszeń w dwukierunkowym ruchu HTTP z włączonymi wszystkimi funkcjami wykrywania zagrożeń
* Proponowane rozwiązanie musi obsługiwać minimum 750 tys . jednoczesnych sesji.
* Proponowane rozwiązanie musi obsługiwać 32000 nowych sesji /s w ruchu HTTP.
 |  |
| Usługi sieciowe | * Musi obsługiwać pasywny tryb pracy (TAP), nie ingerując w sieć klienta.
* Rozwiązanie musi być w stanie zintegrować się z zaporami ogniowymi tej samej marki w celu ograniczenia zagrożeń
* Musi posiadać możliwosc rozwiązywania wiadomości przez protokół MPLS oraz VXLAN i wykrywania zagrożeń w tych wiadomościach.
 |  |
| Kontrola aplikacji | * Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka oraz wspierać komunikatory internetowe, p2p, pocztę e-mail, przesyłanie plików, gry online, strumieniowe przesyłanie multimediów itp.
* Rozwiązanie musi być w stanie zidentyfikować aplikacje mobilne typu iOS lub Android.
* Rozwiązanie musi być w stanie identyfikować aplikacje w chmurze, musi zapewniać wielowymiarowe monitorowanie i statystyki dla aplikacji w chmurze, w tym kategorię ryzyka i funkcje.
 |  |
| Wykrywanie zagrożeń | * Rozwiązanie musi obsługiwać co najmniej 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, ręczne i automatyczne aktualizacje, wyodrębnianie sygnatur oraz wbudowaną encyklopedię zagrożeń.
* Rozwiązanie musi obsługiwać ochronę przed atakami SQL injection, XSS, buffer overflow
* Rozwiązanie powinno obsługiwać ochronę przez atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, Musi obsługiwać wykrywanie co najmniej metod uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA
* Rozwiązanie musi obsługiwać wykrywanie anomalii protokołów HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS itp.
* Niestandardowe reguły wykrywania włamań muszą obsługiwać konfigurowanie kierunku ruchu ataku w celu poprawy dokładności analizy źródła ataku.
* Rozwiązanie powinno umożliwiać tworzenie białych list dla modułu IPS.
* Rozwiązanie musi mieć wstępnie zdefiniowane profile IPS.
* Rozwiązanie musi mieć opcję przechwytywania pakietów
* System musi mapować wykryte zagrożenia na framework MITRE ATT&CK
 |  |
| Skanowanie antywirusowe | * Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur.
* Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP.
* Rozwiązanie powinno obsługiwać wykrywanie wirusów w skompresowanych plikach, takich jak RAR, ZIP, GZIP, BZIP2, TAR oraz wspierać wielowarstwowe wykrywanie skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji po wykryciu zagrożenia w tych plikach
* Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików
 |  |
| Wykrywanie botnetów C&C | * Rozwiązanie powinno wspierać skuteczne wykrywanie botów intranetowych i zapobieganie dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównywanie uzyskanych informacji z bazą adresów C&C.
* Rozwiązanie musi obsługiwać automatyczną aktualizację sygnatur botnetów C&C
* Rozwiązanie musi obsługiwać dwa typy bazy adresów C&C: bazę adresów IP i bazę danych domen.
* Rozwiązanie musi obsługiwać wykrywanie C&C protokołów w protokołach TCP, HTTP i DNS.
* Rozwiązanie musi wspierać właczenie wykrywania DGA w celu analizy odpowiedzi DNS i wykrywania, czy urządzenie jest atakowane przez nazwę domeny DGA.
* Musi wspierać wykrywanie tunelowania w protokole DNS w tym analizowanie zapytań DNS a także rejestrować logów zagrożeń wykrytych tuneli DNS.
 |  |
| Sandbox w chmurze | * Rozwiązanie musi obsługiwać oparte na chmurze wirtualne środowisko analizy złośliwego oprogramowania w celu znalezienia nieznanych zagrożeń
* Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do piaskownicy w chmurze w celu analizy.
* Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów, w tym HTTP/HTTPS, POP3, IMAP4, SMTP i FTP.
* Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR , SWF oraz skrypty
* Rozwiązanie powinno dostarczyć kompletny raport analizy behawioralnej dla złośliwych plików.
* Rozwiązanie musi obsługiwać globalne udostępnianie informacji o zagrożeniach, aby wykryć nowe nieznane zagrożenie.
 |  |
| Wykrywanie spamu | * Rozwiązanie musi wspierać klasyfikację i wykrywanie spamu w czasie rzeczywistym
* Rozwiązanie musi obsługiwać wykrywanie spamu niezależnie od języka, formatu lub treści wiadomości.
* Rozwiązanie musi obsługiwać protokoły poczty e-mail smtp i pop3
* Rozwiązanie musi obsługiwać białe listy wiadomości e-mail z zaufanych domen.
 |  |
| Dodatkowe funkcje ochrony | * Rozwiązanie musi obsługiwać wykrywanie DoS / DDoS, SYN Flood, DNS query flood itp.
* Rozwiązanie musi obsługiwać wykrywanie ataków ARP w tym spoofing ARP
* Rozwiązanie musi obsługiwać wykrywanie anormalnych ataków protokołu.
* Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu pop
 |  |
| Inteligentne funkcje bezpieczeństwa | * Rozwiązanie powinno obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowym zachowaniem i zachowaniem aplikacji, aby wykryć potencjalne zagrożenia lub ataki.
* Rozwiązanie powinno umożliwiać aktualizację bazy danych modelu zachowania szkodliwego oprogramowania online w czasie rzeczywistym.
* Rozwiązanie powinno obsługiwać wykrywanie ponad 2000 znanych i nieznanych rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów itp
* Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na obserwacji zachowania
* Rozwiązanie musi wspierać wykrycia oprogramowania ransomware i złośliwego oprogramowania do wydobywania kryptowalut.
* Rozwiązanie powinno obsługiwać modelowanie zachowania w oparciu o ruch bazowy L3-L7, aby ujawnić nietypowe zachowanie sieci, takie jak skanowanie HTTP, Spider, SPAM, słabe hasła SSH / FTP dla serwerów i hostów.
* Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, reflect, dns query, SSL DDos i aplikacyjny DDoS
* Rozwiązanie musi obsługiwać inspekcję zaszyfrowanego ruchu tunelowego dla nieznanych aplikacji
* Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online w czasie rzeczywistym
* Rozwiązanie musi zapewniać analizę kryminalistyczną , w tym analizę zagrożeń, bazę wiedzy, historię i topologię zagrożeń.
* Rozwiązanie musi obsługiwać działania administratora w celu zmiany stanu zagrożenia na false positive, naprawionego, zignorowanego, potwierdzonego zdarzenia
* Rozwiązanie musi obsługiwać czyszczenie zagrożeń serwera jednym kliknięciem i ponowną ocenę bezpieczeństwa hosta
* Rozwiązanie powinno obsługiwać białą listę zagrożeń, w tym nazwę zagrożenia, źródłowy/docelowy adres IP, liczbę odwiedzin itd.
* Rozwiązanie musi obsługiwać przechwytywanie pakietów online
* Rozwiązanie musi obsługiwać lokalną technologię honeypot, aby wychwytywać ataki zagrożeń sieciowych i potwierdzać źródło zagrożenia, typ zagrożenia i częstość występowania
* Rozwiązanie musi obsługiwać wykrywanie oszustw na podstawie behawioralnej dla ftp, HTTP, MYSQL, SSH, TELNET, dokumentów lub baz danych
* Rozwiązanie musi obsługiwać funkcję polowania na zagrożenia (threat hunting), aby zebrać kompleksowe dowody i zapewnić dogłębną analizę
* Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force remote dekto, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu poprawy wykrywalność funkcji śledzenia zagrożeń.
 |  |
| Widoczność ryzyka/zagrożeń | * Rozwiązanie musi obsługiwać wizualizację zagrożeń intranetowych dla serwerów (zasobów krytycznych), a także wykrywanie nietypowego ruchu z nimi związanego.
* Rozwiązanie musi obsługiwać widoczność zagrożeń dla ryzykownych hostów, w tym nazwy hosta, systemu operacyjnego, przeglądarki, typu usługi, aby rejestrować zagrożenia hosta i nietypowy ruch.
* Rozwiązanie musi obsługiwać widoczność podstawowych informacji opartych na hoście, indeksu ryzyka, zagrożeń i nietypowego ruchu.
* Rozwiązanie powinno wspierać widoczność zagrożeń, w tym nazwę zagrożenia, typ zagrożenia, poziom ryzyka, bazę wiedzy, pakiet kryminalistyczny itp.
* Rozwiązanie powinno dostarczyć wszystkie statystyki klasyfikacji zdarzeń zagrożeń w oparciu o IOC i trend zdarzeń zagrożeń w ciągu co najmniej 2 tygodni.
* Rozwiązanie musi wspierać wskazanie ścieżki ataku.
 |  |
| Analiza i odpowiedzi na incydenty | * Rozwiązanie musi obsługiwać aktualizację w czasie rzeczywistym najpoważniejszych informacji o zagrożeniach znalezionych w branży do urządzenia z chmury
* Obsługa wyświetlania najnowszych informacji o zagrożeniach w wyskakujących okienkach.
* Obsługa rejestrowania i sprawdzania, czy w sieci wystąpiło odpowiednie zagrożenie.
* Pomoc techniczna w celu dostarczenia szczegółowych informacji o zagrożeniach i sugestii dotyczących rozwiązania.
* Wsparcie konfigurowania reguł ostrzegania o zagrożeniach, w tym warunków zagrożenia i metody działania, które w przypadku wystąpienia zdarzenia stanowiącego zagrożenie, system powiadomi użytkownika lub podejmie odpwiedź w odpowiednim czasie zgodnie z metodą działania określoną w regule (np. połączenie z firewall, przypomnienie głosowe lub wysłanie pocztą e-mail.
 |  |
| Administracja | * Rozwiązanie musi mieć zintegrowany sieciowy interfejs użytkownika (WebUI) i interfejs wiersza poleceń (CLI)
* Rozwiązanie powinno obsługiwać zarządzanie dostępem z HTTP/HTTPS, SSH, telnet, konsoli
* Rozwiązanie musi być w stanie chronić system przed atakami brute-force na nazwę użytkownika i hasło
* Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów.
* Rozwiązanie musi obsługiwać monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikując nazwę, system operacyjny, przeglądarkę, typ i rejestr statystyk zagrożeń sieciowych
* Oferowany zestaw urządzeń musi pochodzić o jednego producenta i być w pełni kompatybilny
* Oferowany zestaw urządzeń musi posiadać aplikację mobilną pozwalającą na monitoring pracy urządzeń i analizę zdarzeń
 |  |
| Logowanie i raportowanie | * Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Raport można wyeksportować co najmniej w formacie PDF i/lub wysłać na adres e-mail lub FTP.
* Rozwiązanie powinno obsługiwać ustawianie alarmów dotyczących wykorzystania procesora, wykorzystania pamięci, wykorzystania miejsca na dysku, nowych połączeń itp.
* Rozwiązanie powinno obsługiwać wysyłanie alarmów przez e-mail, SMS.
* Alerty powinny być generowane na podstawie przepustowości aplikacji i nowych połączeń.
* Logi powinny być możliwe do eksportu za pośrednictwem Syslog lub poczty e-mail i zawierać minimum logi zdarzeń, sieci, zagrożenia, konfigurację i sesje
* Wstępnie zdefiniowane zadania raportowania
* Rozwiązanie powinno mieć scentralizowane monitorowanie wielu urządzeń, w tym procesora, pamięci, ruchu, sesji, aplikacji, użytkowników, zagrożeń itp. za pośrednictwem aplikacji mobilnej z danymi z ostatnich 7 dni.
* Rozwiązanie musi wspierać restAPI
 |  |
| Gwarancja i dostawa | * Dostawa musi zawierać również:
* 48-miesięczną gwarancję producenta na dostarczone elementy systemu
* Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 48 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)
* Wsparcie techniczne dystrybutora rozwiązań w języku polskim
* System wizyjny min. 50 cali
 |  |

1. **Urządzenie UTM**

|  |  |  |
| --- | --- | --- |
| Parametr  | Charakterystyka  | Oferowany parametr |
| Wymagania ogólne w zakresie dostawy sprzętu. | * Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
* Dostarczony sprzęt musi być fabrycznie nowy (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu.
* Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.
* Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów.
* Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
 |  |
| 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• Możliwość stworzenia minimum 128 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q.• W zakresie Firewall, obsługa nie mniej niż 1 500 000 jednoczesnych połączeń i 130 000 nowych połączeń na sekundę.• System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o minimalnej pojemności 8 GB do celów logowania i raportowania.• Możliwość rozszerzenia pamięci do 2 TB poprzez dodatkowy dysk SSD bez otwierania obudowy urządzenia• Musi posiadać 2x USB 3.0 z przodu urządzenia• System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu.• System musi mieć możliwość włączenia min 1 systemu wirtualnego bez dodatkowej licencji i możliwości rozszerzenia do minimum 5 poprzez dodatkową licencję w przyszłości• Systemy wirtualne muszą obsługiwać QOS• System pełniący funkcję zapory musi posiadać nie mniej niż: 2x SFP+, 8x SFP, 8x GE interfejsów• Urządzenie musi posiadać dedykowany port przeznaczony do zarządzania |  |
| Funkcjonalności: | • Kontrola dostępu — zapora sieciowa Stateful Inspection• Ochrona przed wirusami - komercyjny antywirus [AV]• Poufność danych - IPSec VPN i SSL VPN• Kontrola witryn sieci Web — filtr URL• Kontrola zawartości poczty - antyspam (dla protokołów SMTP, POP3)• 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• Kontrola aplikacji i rozpoznawanie ruchu P2P (wideo, gry itp.) oraz ograniczanie nowych połączeń i jednoczesnych sesji• Reputacja IP• Cloud Sandbox |  |
| Wydajność: | • Analiza ruchu szyfrowanego protokołem SSL• Wydajność Firewall co najmniej 10 Gb/s• Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym IPS i kontrolą aplikacji 3 Gb/s• Wydajność ochrony przed atakami (IPS) minimum 5Gb/s• Wydajność AV nie mniej niż 4Gb/s• Inspekcja SSL Proxy nie mniejsza niż 800Mbps• Wydajność skanowania z włączoną kontrolą aplikacji, AV, IPS, filtrem URL nie mniejsza niż 2Gbps. |  |
| Funkcjonalności VPN: | • Wydajność IPSec VPN, nie mniej niż 5 Gb/s• Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja• Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem.• Monitorowanie stanu tuneli VPN i utrzymywanie ich aktywności• Praca w toplogiach Hub and Spoke i Mesh• Wspierane mechanizamy : IPSec NAT Traversal, DPD, Replay Detection, Xauth, DHCP over IPsec,• Wsparcie grup DH dla IKEv1: 1,2,5,19,20,21,24• Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,19,20,21,24• Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance)• 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• Obsługa Policy Based Routing• Funkcjonalność Virtual Wire |  |
| Translacja adresów NAT: | • Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego.• Obsługa NAT46, NAT64, DNS64• Wsparcie dla STUN |  |
| 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).• Możliwość budowania min. 12000 polityk• Musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego• 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• Musi mieć możliwość konfiguracji oddzielnych wirtualnych routerów• Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników |  |
| Ochrona antywirusowa: | • Silnik antywirusowy musi być oparty na przepływie tzw. flow-based• Musi umożliwiać skanowanie protokołów HTTP, SMTP, POP3, IMAP, FTP / SFTP, SMB• Możliwość ręcznego dodawania lub usuwania sygnatury MD5 do bazy danych AV• 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 |  |
| Równoważenie obciążenia: | • Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łącza dla określonej nazwy domeny oraz monitorowanie stanu łącza poprzez aktywną metodę wykrywania• Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted leastconnection i weighted round-robin• Kontrola stanu serwera, monitorowanie sesji i ochrona sesji |  |
| Ochrona IPS: | * Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury.
* Baza danych wykrytych ataków musi zawierać co najmniej 12000 sygnatur. Dodatkowo musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i Ddos.
* Funkcjonalność zapobiegania atakom SQL injection, XSS injection
* Możliwość budowania własnych niestandardowych reguł IPS
 |  |
| Obrona przed atakiem: | * Ochrona przed nieprawidłowym działaniem protokołu
* Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment itp.
* Wsparcie IPv4 jak i IPv6 dla ochrony przed DNS query flood i DNS reply flood
* Biała lista docelowych adresów IP
 |  |
| Ochrona antyspam | * Rozwiązanie musi zapewniać ochronę przed spamem w czasie rzeczywistym
* Wspieranymi protokołami są minimum SMTP, SMTPS, POP3, POP3S
* Skanowanie antyspamowe musi odbywać się w ruchu w obu kierunkach
* Musi istnieć możliwość dodawania wyjątków w zakresie skanowania antyspamowego, minimum białych list domen
 |  |
| 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
* Baza danych aplikacji zawierająca ponad 4700 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka
 |  |
| Filtr adresów URL: | * Baza filtrów URL pogrupowana w co najmniej 64 kategorie tematyczne. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków.
* Możliwość zdefiniowania własnej bazy kategorii www.
* Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL.
* Kategoria takie jak hazard, malware, spam, botnety
* Obsługa Safe Search
* Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne
* Dostosowanie strony ostrzeżenia
 |  |
| Ochrona danych: | * Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy
* Identyfikacja protokołu pliku, w tym HTTP,FTP、SMTP, POP3、IMAP
* Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS
* 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
* 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
* Wsparcie DNS sinkhole
* Wsparcie wykrywania tunelowania DNS
* Wyrywanie i blokowanie DGA
 |  |
| Cloud Sandbox: | * Złośliwe oprogramowanie emulowane w wirtualnym środowisku oparte na architekturze chmury w celu wykrywania nieznanych zagrożeń
* 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
* Obsługa blokowania wyników wykrywania w celu szybkiego blokowania nieznanych zagrożeń
 |  |
| Uwierzytelnianie użytkownika: | * System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika z nie mniej niż:
	+ Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu
	+ Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP
	+ Hasła dynamiczne (RADIUS) oparte o zewnętrzne bazach danych
	+ Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA
* Musi umożliwiać budowę architektury uwierzytelniania pojedynczego logowania w środowisku Active Directory
* Wsparcie usług terminalowych
* Uwierzytelnianie użytkownika przez Web przed dostępem do internetu
* Obsługa dwuskładnikowego uwierzytelniania, 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
* W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż:
	+ Posiadanie predefiniowanych raportów dla ruchu internetowego, modułu IPS, skanera antywirusowego i antyspamowego
	+ Generowanie co najmniej 10 rodzajów raportów
 |  |
| 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: | * posiadać certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSA Labs dla funkcji Firewall
* być pozycjonowanym w raporcie Gartnera przez ostatnie 8 lat
 |  |
| 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.
* Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI bez instalowania oddzielnego oprogramowania, takiego jak dedykowana konsola
 |  |
| Gwarancja i dostawa | Dostawa musi zawierać również:* 60-miesięczną gwarancję producenta na dostarczone elementy systemu
* Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 60 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)
* Wsparcie techniczne dystrybutora rozwiązań w języku polskim
* Oferta musi być złożona przez autoryzowanego partnera
 |  |

1. **Swich zarządzalny sztuk 4.**

|  |  |  |
| --- | --- | --- |
| Parametr  | Charakterystyka  | Oferowany parametr |
| Dane techniczne  | Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:* Ilość portów 48 porty 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne
* Chłodzenie od przodu do tyłu obudowy
* Możliwość instalacji redundantnego zasilacza
* Tablica MAC min. 16K
* Tablica ARP/NDP min. 888
* Bufor 16Mb
* MTBF min. 578472 godzin
* Wydajność min. 130,9 Mp/s
* Przepustowość min. 176 Gb/s
* Port USB
* Port miniUSB
* Port zarządzania Out-of-band;
* Web GUI
* HTTPs
* CLI
* Telnet
* SSH
* SNMP
* MIB RSPAN
* Radius
* TACACS+
* DiffServ
* Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
* IPv4/IPv6 Multicast filtering
* IGMPv3 MLDv2 Snooping
* ASM & SSM
* IGMPv1,v2 Querier
* Auto-VoIP
* Auto-iSCSI
* Policy-based routing (PBR)
* LLDP-MED
* Spanning Tree
* Green Ethernet
* STP
* MTP
* RSTP
* PV(R)STP
* BPDU/STRG Root Guard
* EEE (802.3az)
* GVRP/GMRP
* Q in Q,
* Private VLAN
* DOT1X
* MAB
* Captive Portal
* DHCP Snooping
* Dynamic ARP
* Inspection
* IP Source Guard
* CPU min 800 Mhz
* Min 1GB RAM
* Min 256MB Flash
* Min ilość obsługiwanych VLAN 4K
* DHCP Server min 2K rezerwacji
* sFlow
* Minimalna ilość przełączników w stosie: 8
* Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s
* Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
* Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
* Non-stop forwarding (NSF)
* Distributed Link Aggregation (LAGs across the stack)
* Ilość interfejsów IP 128
* Double VLAN Tagging (QoQ)
* PIM-DM (Multicast Routing - dense mode)
* PIM-DM (IPv6)
* PIM-SM (Multicast Routing - sparse mode)
* PIM-SM (IPv6)
* RIPv1
* RIPv2
* OSPFv2
* RFC 2328
* RFC 1583
* OSPFv3
* OSPFv2 min. sąsiadów 400
* OSPFv3 min. sąsiadów 400
* OSPFv3 min. sąsiadów na interfejs 100
* UDLD
* LLPF
* DHCPv6 Snooping
* wysyłanie alertów na email
* MMRP
* Ilość ACL min. 100
* Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu
* Zasilacz z certyfikatem 80+
* CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014,
* Class A, EN 61000-3-3:2013, EN 55024:2010
* VCCI : VCCI-CISPR 32:2016, Class A
* RCM: AS/NZS CISPR 32:2013 Class A
* FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014
* ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014
* BSMI: CNS 13438 Class A
 |  |