



McAfee IntruShield — sieciowy system zapobiegania włamaniom

Pionierskie, przodujące na rynku, rozwiązanie nowej generacji zapobiegające włamaniom do sieci.

Wyzwanie

Zagrożenia bezpieczeństwa przedsiębiorstw i usługodawców stale narastają, w miarę jak rośnie z roku na rok liczba luk w zabezpieczeniach oraz szybkość i stopień wyrafinowania ataków wykorzystujących takie luki. Rozwój nowych ataków hybrydowych, które wykorzystują więcej niż jedną metodę łamania zabezpieczeń oznacza, że przedsiębiorstwa muszą bronić się przed stale zmieniającym się zagrożeniem.

- **Dynamiczne zagrożenia bezpieczeństwa** — Dynamiczny charakter współczesnych zagrożeń bezpieczeństwa oznacza, że nowe ataki hybrydowe nasilają się w niespotykanym dotąd tempie. Luki w zabezpieczeniach sieci powodują, że zasoby o znaczeniu krytycznym są narażone na ataki oraz zwiększa się zagrożenie bezpieczeństwa przedsiębiorstw i usługodawców.
- **Niedostateczna ochrona za pomocą tradycyjnych technologii zabezpieczeń** — Pomimo znacznych nakładów na ochronę, przedsiębiorstwa w dalszym ciągu są narażone na zaawansowane ataki klasy „zero-day”, gdyż tradycyjne technologie nie umożliwiają prewencyjnego wykrywania zagrożeń i zapobiegania im.
- **Potrzeba prewencyjnej ochrony przed zagrożeniami** — Obecnie nie istnieje żaden produkt, który chroniłby przed wszystkimi zagrożeniami. W celu zapewnienia kompleksowej ochrony, usługodawcy i przedsiębiorstwa powinni zastosować podejście wielowarstwowe, które umożliwi prewencyjną ochronę przed zagrożeniami polegającą na precyzyjnym wykrywaniu i blokowaniu zarówno ataków znanych, jak i nieznanymi klasy „zero-day”, zanim spowodują one jakiegokolwiek szkody.

Pionierskie i sprawdzone rozwiązanie firmy McAfee® do zapobiegania włamaniom zapewnia kompleksową, dokładną oraz skalowalną ochronę przed zagrożeniami, pomagając przedsiębiorstwom i usługodawcom zapewnić dostępność oraz bezpieczeństwo infrastruktury sieciowej o znaczeniu krytycznym przez prewencyjne zapobieganie zagrożeniom.

Rozwiązanie McAfee IntruShield

System zapobiegania włamaniom McAfee IntruShield® zapewnia zaawansowaną ochronę w czasie rzeczywistym przed atakami znanymi, klasy „zero-day” (nieznanymi) oraz zaszyfrowanymi, a także przed oprogramowaniem szpiegującym (spyware) czy zagrożeniami związanymi z usługami VoIP. Jest to kompleksowe, dokładne i skalowalne rozwiązanie zapobiegania włamaniom, odpowiednie dla wielu różnych środowisk o znaczeniu krytycznym. Będąc częścią proponowanej przez McAfee strategii Protection-in-Depth™, zapewnia kompleksową prewencyjną ochronę przed włamaniami, pozwalającą na utrzymanie dostępności zasobów biznesowych przedsiębiorstwa i jego infrastruktury sieciowej o znaczeniu krytycznym dzięki wykrywaniu oraz blokowaniu ataków zanim zdążą one wyrządzić jakiegokolwiek szkody. Dzięki szerokiej gamie zintegrowanych urządzeń,

których przepustowość można skalować od setek megabitów do wielu gigabitów na sekundę, rozwiązanie IntruShield chroni wszystkie składniki infrastruktury — od rdzenia, przez brzeg sieci, po biura zdalne, zapewniając skalowalność klasy korporacyjnej i operatorskiej w środowiskach zarówno dużych, jak i małych firm.

Nowatorska architektura IntruShield łączy w sobie opatentowane mechanizmy analizy sygnatur, wykrywania anomalii i ataków typu DDoS („odmowa usługi”), umożliwiając precyzyjne i inteligentne wykrywanie ataków oraz zapobieganie im nawet w przypadku szybkości sięgających kilku gigabitów na sekundę. To bezprecedensowe wykorzystanie nowatorskich technologii umożliwia także zabezpieczanie najbardziej wymagających sieci przed atakami znanymi, nieznanymi klasy „zero-day” i DoS oraz oprogramowaniem szpiegującym. Zastosowana w rozwiązaniu IntruShield technologia nowej generacji zapewnia także po raz pierwszy ochronę przed atakami zaszyfrowanymi oraz integrację systemu zapobiegania włamaniom z zaporą sieciową - firewall. Cechy te sprawiają, że IntruShield jest najdokładniejszym i najbardziej wszechstronnym rozwiązaniem do ochrony sieci dostępnym na rynku.

Rodzina produktów IntruShield obejmuje sześć modeli: IntruShield 4010, IntruShield 4000, IntruShield 3000, IntruShield 2700, IntruShield 1400 oraz IntruShield 1200. Wszystkie są rozbudowanymi, wyspecjalizowanymi urządzeniami zapobiegającymi włamaniom do sieci. Ich wydajność i funkcjonalność spełnia wymagania sieci o wysokiej dostępności w zakresie zapewnienia im bezpieczeństwa. W skład rodziny wchodzi także system IntruShield Security Management — wszechstronne i skalowalne rozwiązanie do zarządzania ochroną sieci.

Cechy i korzyści

Kompleksowa ochrona

- **Ochrona w czasie rzeczywistym przed atakami zaszyfrowanymi** — Pierwsze i jedyne rozwiązanie zapobiegania włamaniom do sieci, które chroni przed atakami niezasyfrowanymi, zaszyfrowanymi oraz oprogramowaniem szpiegującym.
- **Analiza sygnatur, anomalii i ataków typu DoS** — Ochrona przed atakami znanymi, nieznanymi klasy „zero-day” i typu odmowa usługi (DoS, DDoS).
- **System zapobiegania włamaniom i zaporą wewnętrzną** — Niespotykany mechanizm ochrony przed zagrożeniami wewnętrznej infrastruktury systemowej i sieciowej oraz egzekwowania reguł ruchu sieciowego za pomocą funkcji zapory wewnętrznej firewall i systemu zapobiegania włamaniom do sieci.
- **Zintegrowane systemy zapobiegania włamaniom do sieci i hostów** — Przełomowy poziom integracji, dzięki której jedna konsola IntruShield Manager agreguje oraz koordynuje zdarzenia związane z ochroną, generowane przez mechanizmy ochrony hosta (McAfee Enterecept®) i sieci (McAfee IntruShield).

McAfee®

- **Opcje wdrożenia zapewniające wysoką dostępność** — Możliwość wirtualizacji i najlepsza ochrona prewencyjna przed włamaniami dla szerokiej gamy środowisk o wysokiej dostępności.

Dokładna ochrona

- **Dogłębna analiza** — Specjalnie zaprojektowana platforma sprzętowa IntruShield umożliwia analizę ruchu z pamięcią stanu (stateful), obejmującą analizę składni ponad stu protokołów oraz ponad 3 tys. wysokiej jakości sygnatur z wieloma sprawdzeniami i wyzwalaczami. W połączeniu z wysoką odpornością na próby ominięcia zabezpieczeń, zapewnia ona najwyższą dokładność ochrony w czasie rzeczywistym elementów o znaczeniu krytycznym.
- **Wirtualny system zapobiegania włamaniom i zaporą wewnętrzną** — Wyjątkowe funkcje wirtualizacji IntruShield obejmują zarówno mechanizm zapobiegania włamaniom, jak i zaporę wewnętrzną. Dzięki temu reguły ochrony mogą być bardzo szczegółowe i w wysokim stopniu dostosowane do potrzeb użytkownika, co znacznie zmniejsza liczbę fałszywych trafień.
- **Inteligentne wykrywanie włamań** — Rozbudowane funkcje zapewniające szczegółowe, precyzyjne i wiarygodne informacje o włamaniach, ich istotności, kierunku i skutkach, a także ich analizę.

Skalowalność i łatwość zarządzania

- **Skalowalność klasy korporacyjnej** — Dzięki szerokiej gamie rozwiązań, których przepustowość można skalować od setek megabitów do wielu gigabitów na sekundę, IntruShield chroni wszystkie składniki infrastruktury — od rdzenia, przez brzeg sieci, po biura zdalne. Sprawdza się w momentach krytycznych, a jego skalowalność została sprawdzona we wszystkich rodzajach środowisk korporacyjnych.
- **Elastyczność wdrożenia** — Rozwiązanie do zapobiegania włamaniom lub wykrywania włamań może być wdrożone w sposób niezwykle elastyczny. Dostępne tryby — przezroczysty (In-Line), przyłączeniowy (Tap) grupowania portów (Port Clustering), wysokiej dostępności HA oraz nasłuchu Span, mogą znaleźć zastosowanie w każdej architekturze zabezpieczeń sieci.
- **Automatyczne aktualizowanie zagrożeń w czasie rzeczywistym** — Nowatorski, zautomatyzowany proces, który umożliwia aktualizację sygnatur w całym przedsiębiorstwie w czasie rzeczywistym, bez konieczności ponownego uruchamiania urządzeń, oraz zapewnia ochronę przed nowo wykrytymi lukami w zabezpieczeniach, eliminując konieczność ręcznych aktualizacji i przestoje sieci.

Kompleksowa ochrona przed zagrożeniami

Oferta IntruShield, będąca elementem proponowanej przez McAfee strategii Protection-in-Depth, obejmuje kompleksowe rozwiązania do zapobiegania włamaniom, które zapewniają ochronę zarówno wewnętrzną, jak i zewnętrzną infrastruktury sieciowej przed różnymi zagrożeniami i atakami. Ochrona rozciąga się na wszystkie składniki infrastruktury — od rdzenia, przez brzeg sieci, po biura zdalne. Połączenie szeroko zakrojonej ochrony środowiska sieciowego z nowatorskimi technologiami zapobiegania zagrożeniom — takimi jak zapobieganie atakom

IntruShield 4010

Model IntruShield 4010 (I-4010) może być stosowany w sieciach rdzeniowych dużych przedsiębiorstw, w centrach przetwarzania danych bądź w sieciach usługodawców. Interfejsy Gigabit Ethernet o dużej gęstości upakowania portów zapewniają przepustowość i nadmiarowość operacyjną niezbędną do zabezpieczania infrastruktury sieciowej o wysokiej dostępności, a także ekonomię skali wymaganą przez duże przedsiębiorstwa, centra przetwarzania danych i usługodawców.



- Dwanaście portów detekcyjnych Gigabit Ethernet
- Jeden port do zarządzania Fast Ethernet
- Opcjonalny nadmiarowy zasilacz wymieniany podczas pracy
- Specjalizowana platforma sprzętowa zapewniająca wysoką wydajność, wysoką dostępność i małe opóźnienie
- Przepustowość do 2 Gb/s.

IntruShield 4000

Model IntruShield 4000 (I-4000) może być stosowany w sieciach rdzeniowych przedsiębiorstw, w centrach przetwarzania danych bądź w sieciach usługodawców. Interfejsy Gigabit Ethernet zapewniają przepustowość i nadmiarowość operacyjną wymaganą do zabezpieczenia infrastruktury sieciowej o wysokiej dostępności.



- Cztery porty detekcyjne Gigabit Ethernet
- Jeden port do zarządzania Fast Ethernet
- Opcjonalny nadmiarowy zasilacz wymieniany podczas pracy
- Specjalizowana platforma sprzętowa zapewniająca wysoką wydajność, wysoką dostępność i małe opóźnienie
- Przepustowość do 2 Gb/s.

IntruShield 3000

Model IntruShield 3000 (I-3000) może być stosowany w sieci rdzeniowej dużych przedsiębiorstw, w centrach przetwarzania danych bądź w sieciach usługodawców. Interfejsy Gigabit Ethernet o dużej gęstości upakowania portów zapewniają przepustowość i nadmiarowość operacyjną wymaganą do zabezpieczenia infrastruktury sieciowej o wysokiej dostępności, a także ekonomię skali wymaganą przez duże przedsiębiorstwa, centra przetwarzania danych i usługodawców.



- Dwanaście portów detekcyjnych Gigabit Ethernet
- Jeden port do zarządzania Fast Ethernet
- Opcjonalny nadmiarowy zasilacz wymieniany podczas pracy
- Specjalizowana platforma sprzętowa zapewniająca wysoką wydajność, wysoką dostępność i małe opóźnienie
- Przepustowość do 1 Gb/s.



zaszyfowanym i integracja z zaporą wewnętrzną — powoduje, że IntruShield ustanawia nowy standard zapobiegania włamaniom oraz zapewnia kompleksową ochronę przed atakami znanymi, klasy „zero-day” oraz zaszyfowanymi, a także przed oprogramowaniem szpiegującym czy zagrożeniami związanymi z VoIP.

Zapobieganie atakom zaszyfowanym

Informacja, która wymaga ochrony protokołem SSL, ma zazwyczaj znaczenie krytyczne. W dzisiejszym środowisku, nacechowanym dynamicznie zmieniającymi się zagrożeniami, całkowicie dostępny i niezabezpieczony protokół HTTP jest jednym z najczęściej używanych przez hakerów do przeprowadzania ataków. Ochrona ważnych danych znajdujących się na samym serwerze WWW jest bardzo ważna, ale współczesne witryny handlu elektronicznego mają także dostęp do informacji przechowywanych w serwerach baz danych działających w warstwie rdzeniowej sieci.

Ochrona infrastruktury korzystającej z protokołu SSL ma kluczowe znaczenie dla zapewnienia bezpieczeństwa danych na lokalnym serwerze WWW, a także dla eliminowania potencjalnych dróg ataku na zaufaną sieć wewnętrzną. Przełomowa technologia zapobiegania włamaniom IntruShield zapewnia kompleksową ochronę sieci przed atakami zarówno niezasyfowanymi, jak i zaszyfowanymi. W rozwiązaniu tym zastosowano rewolucyjne podejście polegające na deszyfrowaniu i analizowaniu ruchu SSL, które radykalnie zwiększa zakres ochrony sieci przez prewencyjne wykrywanie i blokowanie szyfrowanych zagrożeń.

- **Kontrola ruchu SSL** — Technologia IntruShield do kontroli ruchu SSL z akceleracją sprzętową umożliwia urządzeniom kopiowanie, deszyfrowanie i kontrolowanie strumienia danych SSL za pomocą bezpiecznie przechowywanego klucza prywatnego SSL. Po konwersji strumienia danych SSL wewnątrz urządzenia do postaci jawnej, ruch jest analizowany przez mechanizmy IntruShield służące do wykrywania anomalii protokołów i aplikacji, mechanizmy analizy statystycznej ataków typu DoS oraz mechanizmy analizy sygnatur. Jeśli nie zostanie wykryty atak, oryginalny zaszyfowany pakiet jest przesyłany dalej z minimalnym tylko opóźnieniem.
- **Zapobieganie zaszyfowanym atakom na SSL** — Stosowana w IntruShield ochrona przed zagrożeniami zaszyfowanymi polega na odrzuceniu pakietów uznanych za szkodliwe w momencie wykrycia ataku.
- **Rejestracja ataków na SSL dla celów sądowych** — Urządzenie IntruShield może być tak skonfigurowane, aby przechwytywał i przechowywał w programie IntruShield Manager zdeszyfrowane kopie pakietów SSL, w których wykryty został atak. Przechwycone pakiety są przesyłane z urządzenia do programu IntruShield Manager przez połączenie szyfrowane.
- **Pełne bezpieczeństwo kluczy SSL** — Ochrona klucza prywatnego SSL ma podstawowe znaczenie dla zapewnienia bezpieczeństwa. W celu zagwarantowania poufności i integralności klucza prywatnego, jest on w bezpieczny sposób eksportowany w formacie zaszyfowanym do programu IntruShield Manager. Tam następuje jego ponowne szyfrowanie za pomocą klucza publicznego docelowego urządzenia i w tej formie klucz jest przechowywany lokalnie. Podczas przeprowadzania

IntruShield 2700

Model IntruShield 2700 (I-2700) to elastyczny system zapobiegania włamaniom, przeznaczony do stosowania na obrzeżach sieci przedsiębiorstwa. Interfejsy Fast Ethernet i Gigabit Ethernet efektywnie chronią wiele segmentów sieci.



- Dwa porty detekcyjne Gigabit Ethernet i sześć portów detekcyjnych Fast Ethernet
- Wbudowane przyłącza TAP do sieci Fast Ethernet
- Jeden port do zarządzania Fast Ethernet
- Specjalizowana platforma sprzętowa zapewniająca wysoką wydajność, wysoką dostępność i małe opóźnienie
- Przepustowość do 600 Mb/s.

IntruShield 1400

Model IntruShield 1400 (I-1400) to ekonomiczny system zapobiegania włamaniom przeznaczony do stosowania w sieciach średniej wielkości, w sieciach zdalnych biur i oddziałów lub na obrzeżach sieci przedsiębiorstwa. Dzięki scentralizowanemu zarządzaniu przez Internet wszystkimi rozwiązaniami do zapobiegania włamaniom wdrożonymi w przedsiębiorstwie, znacznie obniża koszty eksploatacji.



- Cztery porty detekcyjne Fast Ethernet
- Wbudowane przyłącza TAP do sieci Fast Ethernet
- Jeden port do zarządzania Fast Ethernet
- Specjalizowana platforma sprzętowa zapewniająca wysoką wydajność, wysoką dostępność i małe opóźnienie
- Przepustowość do 200 Mb/s.

IntruShield 1200

Model IntruShield 1200 (I-1200) to ekonomiczny system zapobiegania włamaniom przeznaczony do stosowania w sieciach średniej wielkości lub w sieciach zdalnych biur i oddziałów. Dzięki scentralizowanemu zarządzaniu przez Internet wszystkimi rozwiązaniami do zapobiegania włamaniom wdrożonymi w przedsiębiorstwie, znacznie obniża koszty eksploatacji.



- Dwa porty detekcyjne Fast Ethernet
- Wbudowane przyłącza TAP do sieci Fast Ethernet
- Jeden port do zarządzania Fast Ethernet
- Specjalizowana platforma sprzętowa zapewniająca wysoką wydajność, wysoką dostępność i małe opóźnienie
- Przepustowość do 100 Mb/s.

McAfee®

kontroli ruchu SSL, urządzenie IntruShield w bezpieczny sposób przechowuje klucz prywatny SSL w pamięci ulotnej. Gwarantuje to, że niezasyfrowana kopia klucza nie jest nigdzie w systemie przechowywana w sposób trwały.

System zapobiegania włamaniom i zaporą wewnętrzną

Obecne zapory firewall zapewniają ochronę brzegów sieci. IntruShield to pionierskie rozwiązanie w technologii nowej generacji, w którym funkcje wewnętrznej zapory firewall i zapobiegania włamaniom do sieci są zintegrowane w ramach jednej wyspecjalizowanej platformy, po raz pierwszy zapewniającej pełną ochronę sieci wewnętrznej. Taka integracja umożliwia uzyskanie wyższego poziomu ochrony, jednocześnie zapewniając wszechstronne możliwości kontroli, elastyczność oraz obniżenie kosztów posiadania.

Technologia wirtualizacji IntruShield obejmuje zarówno funkcje zapobiegania włamaniom, jak i funkcje wewnętrznej zapory firewall. Dzięki temu klienci po raz pierwszy mogą zaimplementować wirtualną strefę zdemilitaryzowaną wokół zasobów o znaczeniu krytycznym, zapewniając w ten sposób dodatkową warstwę ochrony przed atakami, które przedostają się przez zapory na brzegach sieci lub pochodzą z sieci wewnętrznej. Wirtualne strefy zdemilitaryzowane mogą być konfigurowane z dużą szczegółowością, co pozwala ochronić poszczególne segmenty sieci, wybrane hosty, a nawet pojedyncze systemy przy użyciu specyficznych dla nich reguł.

Analiza sygnatur, anomalii i ataków typu DoS

Opatentowany, zintegrowany mechanizm IntruShield służący do analizy sygnatur, anomalii i ataków typu DoS zapewnia wszechstronną ochronę przed oprogramowaniem szpiegującym oraz atakami znanymi, nieznanymi klasy „zero-day” i DoS. Więcej informacji na ten temat znajduje się w części „Dogłębna analiza” poniżej.

Zintegrowane systemy zapobiegania włamaniom do sieci i hostów

Rozwiązanie firmy McAfee do ochrony przed włamaniami zapewnia niespotykaną integrację produktów IntruShield do zapobiegania włamaniom do sieci oraz produktów Enterccept do zapobiegania włamaniom do hostów. Gwarantuje najlepszą ochronę spośród wszystkich dostępnych na rynku rozwiązań i obejmuje serwery, komputery biurkowe, komputery przenośne oraz warstwę rdzeniową i brzegową sieci.

Precyzja wykrywania

We współczesnym środowisku nacechowanym dynamicznie zmieniającymi się zagrożeniami precyzja wykrywania ma dla operatorów sieci znaczenie podstawowe. Falszywe trafienia systemów wykrywania włamań mogą powodować niepotrzebne alarmy i stanowić utrudnienie dla operatorów, jednak fałszywe trafienia systemów zapobiegania włamaniom są poważniejsze, gdyż mogą blokować uprawniony ruch w sieci. IntruShield umożliwia bardzo precyzyjne wykrywanie ataków, co stanowi podstawę skutecznego rozwiązania do zapobiegania atakom, odpowiedniego do wdrożenia w trybie przezroczystym (in-line) we współczesnych, wymagających środowiskach o znaczeniu krytycznym.

Dogłębna analiza

Dzięki integracji kontekstowej (z pamięcią stanu) analizy sygnatur i anomalii oraz statystycznej analizy ataków typu DoS IntruShield zapewnia doskonałą ochronę przed

oprogramowaniem szpiegującym oraz przed atakami znanymi, nieznanymi klasy „zero-day” i DoS. Analizy te obejmują zarówno ruch niezasyfrowany, jak i zaszyfrowany. Realizowana przez IntruShield analiza ruchu z pamięcią stanu uwzględnia zapamiętane stany obejmujące do miliona sesji, a także dogłębną analizę składniową ponad stu protokołów. Dzięki temu analiza sygnatur, anomalii i ataków typu DoS jest w pełni kompleksowa.

Wykrywanie ataków i zapobieganie im w oparciu o sygnatury

Urządzenia IntruShield zapewniają wydajną analizę sygnatur (zawierają ich ponad 3 tys.), aby zapewnić dokładną ochronę przed znanymi atakami na luki w zabezpieczeniach. Dzięki temu, że rozwiązanie IntruShield koncentruje się na lukach, a nie na pojedynczych atakach, często wykrywa różne warianty ataków bez konieczności dodawania nowych sygnatur.

- **Mechanizm wykrywania sygnatur na podstawie stanu** — Urządzenia IntruShield wykorzystują opatentowany mechanizm wykrywania sygnatur na podstawie stanu. Umożliwia on kontekstowe wykrywanie sygnatur, wykorzystanie zawartych w pakietach danych informacji o stanie, wielokrotne porównywanie tokenów oraz wykrywanie sygnatur ataków, które obejmują więcej niż jeden pakiet bądź są zawarte w nieprawidłowym strumieniu pakietów.
- **Język specyfikacji sygnatur** — Urządzenia IntruShield używają specjalnie opracowanego, wysokopoziomowego języka specyfikacji sygnatur. Architektura IntruShield oddziela sygnatury od oprogramowania urządzenia, dzięki czemu odpowiednie sygnatury mogą być udostępniane w krótszym czasie.
- **Aktualizacja sygnatur w czasie rzeczywistym** — Urządzenia IntruShield wykorzystują innowacyjny proces aktualizacji sygnatur w czasie rzeczywistym, który zapewnia automatyczne pobieranie nowych sygnatur przez oprogramowanie IntruShield Manager zainstalowane w systemie klienta. W zależności od konfiguracji, sygnatury te mogą być automatycznie przesyłane w czasie rzeczywistym z programu IntruShield Manager do urządzeń. Urządzenia IntruShield na bieżąco wykorzystują najnowsze sygnatury bez potrzeby resetowania lub restartowania, przez co zapewniają nieprzerwaną ochronę przed atakami.
- **Sygnatury definiowane przez użytkownika** — Urządzenia mogą także wykorzystywać sygnatury tworzone przez użytkowników za pomocą intuicyjnego graficznego interfejsu programu IntruShield Manager.

Wykrywanie anomalii i zapobieganie im

Wykorzystywane przez urządzenia IntruShield funkcje wykrywania anomalii wykrywają zaawansowane, nieznanne ataki klasy „zero-day”, co znacznie zwiększa wskaźnik wykrywania ataków.

- **Anomalie statystyczne, dotyczące protokołów i aplikacji** — Urządzenia zapewniają kompleksowe wykrywanie anomalii za pomocą technik wykrywania anomalii statystycznych oraz dotyczących protokołów i aplikacji.



- **Wykrywanie przepełnień bufora** — Obecnie ponad połowa ataków polega na wykorzystaniu błędu przepełnienia bufora. Wykorzystując techniki wykrywania anomalii, IntruShield efektywnie chroni przed tym poważnym źródłem zagrożeń.

Wykrywanie ataków typu DoS i zapobieganie im

Rozwiązanie IntruShield zapewnia precyzyjne wykrywanie ataków typu DoS oraz umożliwia prewencyjne ich blokowanie.

- **Samouczące się profile i wykrywanie oparte na wartościach progowych** — Urządzenia umożliwiają wykrywanie ataków typu DoS w oparciu o wartości progowe lub samouczące się profile. Technika ta wykorzystuje opatentowany algorytm, który pozwala wydzielić nawet niewielką liczbę nieprawidłowych pakietów z wielkiej liczby pakietów stanowiących uprawniony ruch i skutecznie blokować ataki typu DoS oraz DDoS.
- **Precyzyjne wykrywanie ataków typu DoS** — Urządzenia zapewniają precyzyjne wykrywanie ataków typu DoS dzięki technikom opartym na profilach. Profil może być utworzony zarówno dla grupy adresów IP, jak i dla pojedynczego hosta. Architektura IntruShield umożliwia obsługę setek profili przez jedno urządzenie. Każde odchylenie od zwykłego zachowania ruchu jest uznawane za atak typu DoS. Atak może zostać wykryty nawet wtedy, gdy wiąże się ze stosunkowo niewielkim ruchem w łączu dosyłowym między pojedynczym hostem (lub pojedynczą podsiecią) a siecią gigabitową.

Wirtualny system zapobiegania włamaniom i zapora wewnętrzna

Urządzenia IntruShield stosują nowatorską, rozbudowaną koncepcję wirtualizacji, która pozwala na ich segmentowanie. Oznacza to, że dla jednego urządzenia IntruShield można zdefiniować nawet tysiąc urządzeń wirtualnych, z których każdy może być niestandardowy (z osobnymi szczegółowymi regułami zabezpieczeń dotyczącymi wykrywania poszczególnych ataków oraz podejmowania odpowiednich działań w reakcji na nie). Urządzenie wirtualne może być zdefiniowane w oparciu o blok adresów IP, jeden lub kilka znaczników VLAN bądź specyficzny port (lub kilka portów) urządzenia.

Wirtualizacja odnosi się zarówno do funkcji zapobiegania włamaniom, jak i zapory wewnętrznej. Ta przełomowa możliwość integracji wirtualnych funkcji zapobiegania

włamaniom i wewnętrznej zapory umożliwia przedsiębiorstwu rozszerzenie ochrony strefy zdemilitaryzowanej na sieć wewnętrzną przy zachowaniu tego samego wysokiego poziomu ochrony. IntruShield umożliwia precyzyjne definiowanie reguł zabezpieczeń dla poszczególnych segmentów sieci, zbioru hostów, a nawet dla pojedynczych adresów IP. Dzięki temu można utworzyć „wirtualną strefę zdemilitaryzowaną” dla chronionych segmentów lub hostów. Technologia IntruShield „wirtualnej strefy zdemilitaryzowanej” (Virtual Perimeter) to pierwsze rozwiązanie na rynku, które zapewnia również ochronę sieci wewnętrznej. Zwiększa ono bezpieczeństwo oraz zapewnia niespotykaną dotąd ochronę sieci wewnętrznych, które często są niezabezpieczone z powodu braku reguł ochrony bądź niedostatecznego ich egzekwowania.

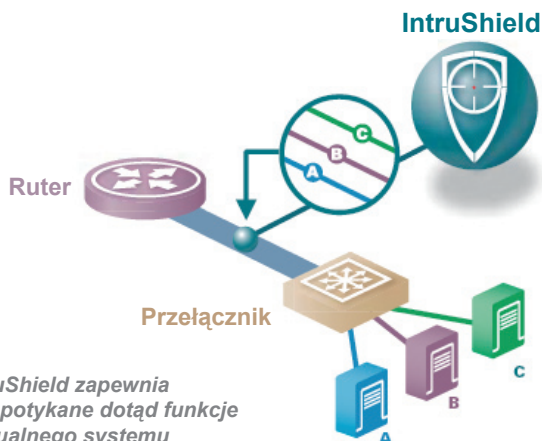
Możliwość wirtualizacji oznacza, że specjaliści ds. bezpieczeństwa sieci mogą implementować i egzekwować zbiór różnych reguł zabezpieczeń w jednym urządzeniu IntruShield. Taka elastyczność pozwala przedsiębiorstwu efektywnie zaspokajać różne potrzeby w zakresie ochrony, natomiast usługodawcom oferować dostosowane rozwiązania ochrony i umowy SLA różnym klientom. Ponadto wirtualizacja dodatkowo zmniejsza liczbę urządzeń wymaganych do wdrożenia w całej sieci oraz obniża całkowity koszt posiadania.

Inteligentne wykrywanie włamań

Dynamiczny charakter współczesnych zagrożeń sprawia, że nowe ataki hybrydowe nasilają się w niespotykanym dotąd tempie. W celu zapewnienia wykrywania i blokowania ataków zarówno znanych, jak i nieznanych klasy „zero-day”, zanim spowodują one jakiegokolwiek szkody, przedsiębiorstwa i usługodawcy powinni przyjąć strategię prewencyjnej ochrony przed zagrożeniami. IntruShield zawiera wyjątkowy zestaw funkcji pod nazwą Intrusion Intelligence™ (Inteligentne wykrywanie włamań), które umożliwiają analizę kluczowych cech zagrożeń i włamań, zarówno znanych, jak i klasy „zero-day”. Te wyjątkowe funkcje zapewniają uzyskanie szczegółowych, dokładnych i wiarygodnych informacji związanych z rozpoznawaniem włamań, określaniem ich istotności, kierunku i skutków oraz służących do ich analizowania. Pozwalają one operatorom i przedsiębiorstwom na przejście od podejścia reaktywnego, polegającego jedynie na wykrywaniu włamań, do podejścia prewencyjnego, które pozwala na blokowanie ataków zanim dotrą one do obiektu, w który zostały wymierzone.

Skalowalność i łatwość zarządzania klasy operatorskiej w całym przedsiębiorstwie

IntruShield zapewnia wyjątkową skalowalność i łatwość zarządzania, odpowiadające potrzebom różnych środowisk korporacyjnych, telekomunikacyjnych i usługodawców. Oferta IntruShield obejmuje pełną gamę platform i rozwiązań, których przepustowość można skalować od setek megabitów do wielu gigabitów na sekundę. Zapewniają one ochronę wszystkich składników infrastruktury — od rdzenia, przez brzeg sieci, po biura zdalne — gwarantując sprawdzoną skalowalność we wszystkich środowiskach sieciowych i sprawdzając się w sytuacjach krytycznych.



IntruShield zapewnia niespotykane dotąd funkcje wirtualnego systemu wykrywania włamań



Ochrona całego przedsiębiorstwa

Modele IntruShield 4010 i IntruShield 4000 zapewniają gigabitową przepustowość i umożliwiają wdrażanie w punktach logicznego agregowania ruchu w rdzeniu sieci przedsiębiorstwa, w centrach przetwarzania danych oraz w sieciach usługodawców. Dzięki wdrożeniu urządzeń przed farmą serwerów, użytkownicy mogą wykorzystać zapewniane przez IntruShield wirtualne funkcje zapobiegania włamaniom (VIPS) do monitorowania każdego punktu agregowania ruchu, przy czym w odniesieniu do każdego aktywnego urządzenia w sieci mogą być zastosowane różne niestandardowe reguły zabezpieczeń. Urządzenia mogą być też wdrożone z opcją wysokiej dostępności HA, która zapewnia przełączanie awaryjne (z zachowaniem pamięci stanu) pomiędzy dwoma urządzeniami bez potrzeby użycia jakiegokolwiek zewnętrznego sprzętu. Zapewnia to nadmiarowość operacyjną, eliminuje punkty podatne na awarię oraz zapewnia ciągłą ochronę przed włamaniami. Model IntruShield 3000, o maksymalnej wydajności 1 Gb/s, to rozwiązanie o wyjątkowo korzystnym wskaźniku cena/wydajność, odpowiednie do wdrożenia w sieci rdzeniowej, sieci operatorskiej oraz u usługodawców. Modele IntruShield 3000 i IntruShield 4010 zapewniają najwyższą gęstość upakowania portów Gigabit Ethernet spośród wszystkich dostępnych na rynku systemów zapobiegania włamaniom do sieci. Model IntruShield 2700, wyposażony w interfejsy Fast Ethernet i Gigabit Ethernet, stanowi elastyczne rozwiązanie dla strefy zdemilitaryzowanej sieci przedsiębiorstwa. Model IntruShield 1400 to skalowalne rozwiązanie dla sieci średniej wielkości, sieci oddziałów, zdalnych biur oraz strefy zdemilitaryzowanej sieci przedsiębiorstwa. Natomiast model IntruShield 1200 jest skalowalnym rozwiązaniem odpowiednim dla sieci średniej wielkości, sieci oddziałów oraz zdalnych biur w sieciach przedsiębiorstw.

Gigabitowa wydajność

Urządzenia IntruShield są oparte na dedykowanych, programowalnych urządzeniach zaprojektowanych z myślą o zapewnieniu bezpieczeństwa i działających w oparciu o system czasu rzeczywistego. Wykrywanie włamań i zapobieganie im to zadania wymagające ogromnej mocy obliczeniowej, osiem do dziesięciu razy większej niż moc obliczeniowa wymagana przez zapory sieciowe. Prawie wszystkie funkcje są wspomagane sprzętowo przez specjalne układy, co pozwala na przyspieszenie o rzędy wielkości powtarzalnych zadań, takich jak analiza protokołów, analiza statystyczna, rozpoznawanie ciągów i wirtualizacja. Dzięki temu urządzenia IntruShield mogą przetwarzać tysiące sygnatur z maksymalną dopuszczalną przez sieć szybkością bez utraty nawet jednego pakietu, zapewniając równocześnie ochronę przed atakami znanymi, nieznanymi klasy „zero-day” i DoS oraz oprogramowaniem szpiegującym czy też zagrożeniom związanym z VoIP. IntruShield to rozwiązanie o nadzwyczaj korzystnym wskaźniku cena/wydajność dla przepustowości od kilkudziesięciu Mb/s do 2 Gb/s.

Elastyczność wdrożenia

Rozwiązanie IntruShield może być elastycznie wdrożone w sieci zapewniając doskonałą ochronę przed zagrożeniami w wielu różnych środowiskach sieci o znaczeniu krytycznym, w tym w trybach: przezroczystym (In-Line), przyłączeniowym (Tap), grupowania portów (Port Clustering), wysokiej dostępności HA oraz nasłuchu Span. IntruShield zapewnia

także kompleksową ochronę infrastruktury, obejmującą routery, przełączniki, wirtualne sieci prywatne oraz bramy.

- Tryb przezroczysty (In-Line) oznacza, że urządzenia IntruShield znajdują się na torze przesyłania danych, przepływający przez nie ruch jest nadzorowany, a — w zależności od szczegółowych reguł — szkodliwe pakiety są blokowane przed dotarciem do celu. Urządzenia IntruShield zapewniają wydajność pozwalającą na pracę bez opóźnień z szybkością fizycznego połączenia które chroni (wire-speed), co zapobiega tworzeniu się w nich wąskich gardeł.
- Tryb grupowania portów (Port Clustering) polega na grupowaniu interfejsów i umożliwia agregowanie ruchu monitorowanego przez wiele portów jednego urządzenia w pojedynczy strumień, poddawany analizie w celu wykrycia ataków uwzględniającego analizę stanu.
- Tryb wysokiej dostępności (High-Availability) i awaryjne przełączanie z zachowaniem pamięci stanu. Urządzenia IntruShield umożliwiają instalację systemu do zapobiegania włamaniom w trybie wysokiej dostępności i przełączanie pomiędzy dwoma urządzeniami w razie awarii jednego z nich.
- Tryb nasłuchu Span polega na tym, że urządzenie monitoruje koncentratory lub porty SPAN wielu przełączników i może inicjować różne działania w reakcji na atak, np. resetowanie sesji TCP w celu zakończenia szkodliwego połączenia przez port monitorujący.
- Tryb przyłączeniowy (Tap) pozwala na pełnodupleksowe monitorowanie i zapewnia widok całego ruchu sieciowego z rozróżnieniem kierunku, co umożliwia analizę ruchu uwzględniającą stany połączenia. Wyznaczone porty reakcyjne umożliwiają podejmowanie pośrednich działań w przypadku ataków, np. resetowanie sesji TCP w celu zakończenia szkodliwego połączenia.



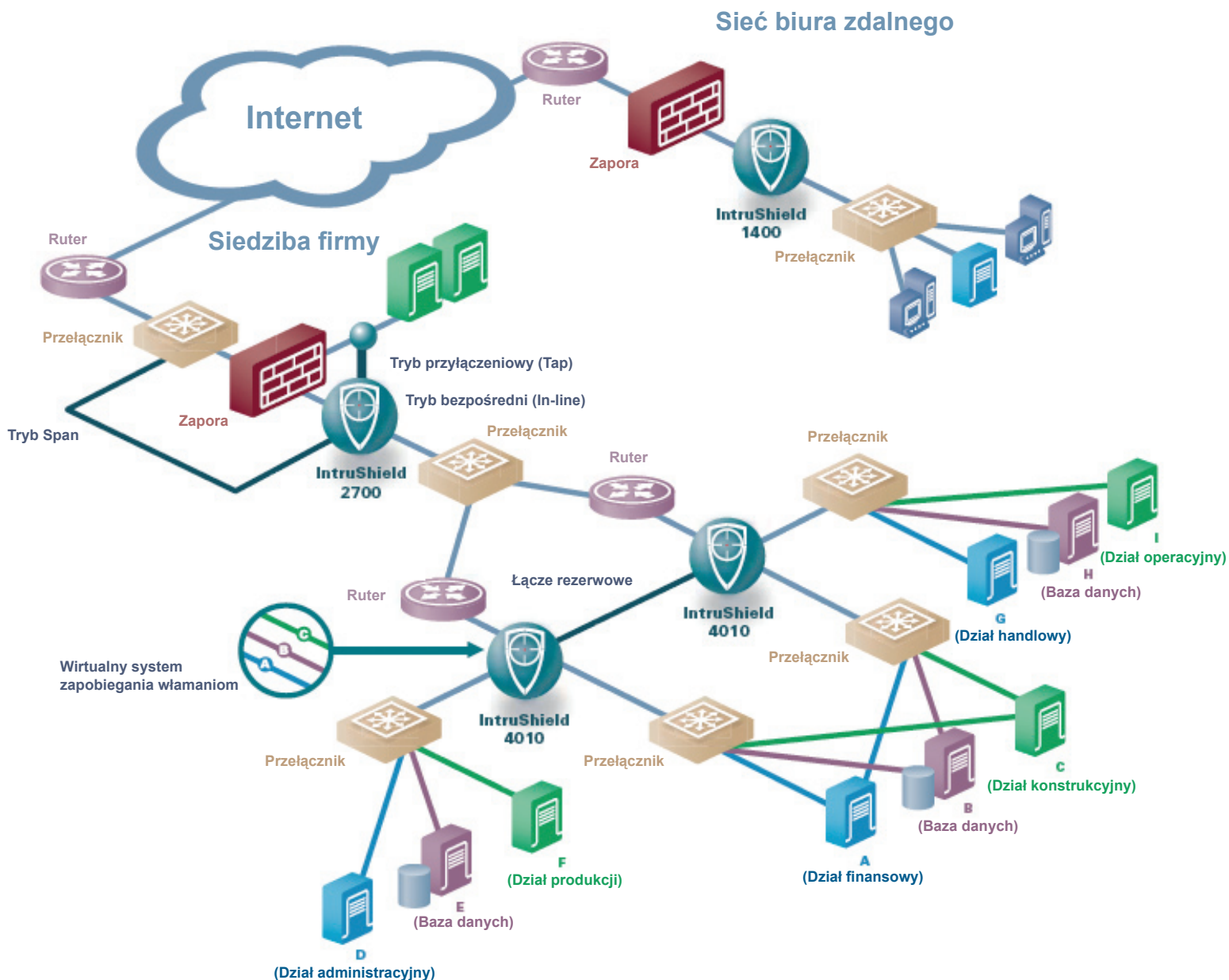
Zapobieganie włamaniom w czasie rzeczywistym

Żaden system zabezpieczeń nie jest kompletny, jeśli nie umożliwia blokowania ataków w czasie rzeczywistym. Precyzyjne ich wykrywanie stanowi podstawę kompletnego zestawu udostępnianych przez urządzenia IntruShield opcji zapobiegania włamaniom w czasie rzeczywistym. Opcje te umożliwiają integrowanie urządzeń IntruShield w środowiskach sieciowych wykorzystujących różne reguły zabezpieczeń — od powiadamiania o atakach w czasie rzeczywistym po pełne ich blokowanie w czasie ich trwania. Po wykryciu ataku urządzenia IntruShield mogą: udaremnić atak w trakcie jego trwania przez odrzucenie albo zablokowanie pakietu lub



sesji; zainicjować resetowanie sesji TCP lub wysłać przez port reakcyjny komunikat ICMP o niemożności osiągnięcia adresata; zmienić konfigurację zapór w taki sposób, aby zablokować ruch naruszający reguły; wysłać alarm do programu IntruShield Manager; powiadomić specjalistów ds. bezpieczeństwa sieci o alarmie za pośrednictwem poczty elektronicznej, pagera lub skryptu; przechwycić i zarejestrować pakiety dla celów bardziej szczegółowej analizy. IntruShield udostępnia pełną gamę reguł zabezpieczeń, które mogą być realizowane nawet przez pojedyncze urządzenie.

Integracja funkcji wykrywania i zapobiegania włamaniom w jednym produkcie umożliwia użytkownikom stopniowe przechodzenie od wykrywania włamań do zapobiegania im, przy jednoczesnej ochronie poczynionych przez przedsiębiorstwo lub usługodawcę inwestycji w technologie.



IntruShield zapewnia niespotykaną elastyczność i skalowalność wdrożenia



Dane techniczne urządzeń IntruShield

Składniki sprzętowe	I-4010	I-4000	I-3000	I-2700	I-1400	I-1200
Lokalizacja sieci	Sieć rdzeniowa	Sieć rdzeniowa	Sieć rdzeniowa	Strefa zdemilitaryzowana	Sieć oddziału; Strefa zdemilitaryzowana	Sieć oddziału
Wydajność/Przepustowość	Do 2Gb/s	Do 2Gb/s	Do 1Gb/s	Do 600 Mb/s	Do 200 Mb/s	Do 100 Mb/s
Maksymalna liczba równoczesnych połączeń	1000 000	1000 000	500 000	250 000	80 000	40 000
Porty						
Porty detekcyjne Gigabit Ethernet	12	4	12	2	-	-
Porty detekcyjne Fast Ethernet (FE)	-	-	-	6	4	2
Wydzielone porty reakcyjne Fast Ethernet (FE)	2	2	2	3	1	1
Wydzielone porty do zarządzania Fast Ethernet (FE)	Tak	Tak	Tak	Tak	Tak	Tak
Zewnętrzne porty sterujące, podtrzymujące połączenie w razie awarii	6	2	6	1	-	-
Porty konsoli i porty dodatkowe	Tak	Tak	Tak	Tak	Tak	Tak
Wbudowane przyłącza sieciowe TAP	Nie	Nie	Nie	Tak <small>(dla portów Fast Ethernet)</small>	Tak	Tak
Otwarcie w razie awarii	Opcjonalnie	Opcjonalnie	Opcjonalnie	Tak <small>(dla portów Fast Ethernet)</small>	Tak	Tak
Zamknięcie w razie awarii	Tak	Tak	Tak	Tak	Tak	Tak
Tryby pracy						
Monitorowanie portów SPAN	Tak	Tak	Tak	Tak	Tak	Tak
Tryb przyłączeniowy (Tap)	Opcjonalnie	Opcjonalnie	Opcjonalnie	Tak <small>(dla portów Fast Ethernet)</small>	Tak	Tak
Tryb przezroczysty (In-Line)	Tak	Tak	Tak	Tak	Tak	Tak
Grupowanie portów (Port Clustering)	Tak	Tak	Tak	Tak	Tak	Tak
Liczba wirtualnych systemów zapobiegania włamaniom VIPS	1 000	1 000	1 000	100	32	16
Monitorowanie ruchu na łączach aktywne-aktywne	Tak	Tak	Tak	Tak	Tak	Tak
Monitorowanie ruchu na łączach aktywne-pasywne	Tak	Tak	Tak	Tak	Tak	Tak
Monitorowanie ruchu asymetrycznego	Tak	Tak	Tak	Tak	Tak	Tak
Funkcje zapewnienia wysokiej dostępności						
Nadmiarowe zasilanie	Tak <small>(Opcjonalnie)</small>	Tak <small>(Opcjonalnie)</small>	Tak <small>(Opcjonalnie)</small>	Tak <small>(Opcjonalnie)</small>	Nie	Nie
Wykrywanie awarii urządzenia	Tak	Tak	Tak	Tak	Tak	Tak
Wykrywanie awarii łącza	Tak	Tak	Tak	Tak	Tak	Tak
Wymiary						
Fizyczne	wysokość 2U, montowane w stelażu 17,44 (szer.) x 3,44 (wys.) x 23,00 (dł.)	wysokość 2U, montowane w stelażu 17,44 (szer.) x 3,44 (wys.) x 23,00 (dł.)	wysokość 2U, montowane w stelażu 17,44 (szer.) x 3,44 (wys.) x 23,00 (dł.)	wysokość 2U, montowane w stelażu 17,44 (szer.) x 3,44 (wys.) x 23,00 (dł.)	wysokość 1U, montowane w stelażu 17,32 (szer.) x 1,65 (wys.) x 10,5 (dł.)	wysokość 1U, montowane w stelażu 17,32 (szer.) x 1,65 (wys.) x 10,5 (dł.)
Waga	ok. 21 kg	ok. 21 kg	ok. 21 kg	ok. 21 kg	ok. 7,7 kg	ok. 6,8 kg
Zasilanie	100-240VAC (50/60Hz)	Takie samo dla wszystkich modeli	Takie samo dla wszystkich modeli	Takie samo dla wszystkich modeli	Takie samo dla wszystkich modeli	Takie samo dla wszystkich modeli
Pobór mocy	350 W	350 W	350 W	250 W	100 W	100 W
Temperatura	0° - 40° C (praca) -40° - 70° (przechowywanie)	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli
Wilgotność względna (bez kondensacji)	Praca: 10% do 90% Przechowywanie: 5% do 95%	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli
Wysokość n.p.m.	0 – 3000 m	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli
Certyfikaty bezpieczeństwa	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, IEC 60825, 21CFR1040Homologacja CB obejmuje wszystkie odstępstwa obowiązujące w poszczególnych krajach.	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli
Certyfikaty EMI	FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Kanada), EN55022 Class A (Europa), CISPR22 Class A (m-narodowe)	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli



Składniki programowe		I-4010	I-4000	I-3000	I-2700	I-1400	I-1200
Kontrola ruchu uwzględniająca analizę stanu.	Defragmentacja ruchu IP i reasemblacja strumienia TCP	Tak	Tak	Tak	Tak	Tak	Tak
	Szczegółowa analiza protokołów	Tak	Tak	Tak	Tak	Tak	Tak
	Monitorowanie ruchu asymetrycznego	Tak	Tak	Tak	Tak	Tak	Tak
	Normalizacja protokołów	Tak	Tak	Tak	Tak	Tak	Tak
	Zaawansowana ochrona przed pomijaniem mechanizmów ochrony	Tak	Tak	Tak	Tak	Tak	Tak
	Gromadzenie danych dla celów sądowych	Tak	Tak	Tak	Tak	Tak	Tak
	Tunelowanie protokołów	Tak	Tak	Tak	Tak	Tak	Tak
Wykrywanie protokołów	Tak	Tak	Tak	Tak	Tak	Tak	
Wykrywanie sygnatur	Sygnatury definiowane przez użytkownika	Tak	Tak	Tak	Tak	Tak	Tak
	Aktualizacja sygnatur w czasie rzeczywistym	Tak	Tak	Tak	Tak	Tak	Tak
Wykrywanie anomalii	Anomalie statystyczne	Tak	Tak	Tak	Tak	Tak	Tak
	Anomalie protokołów	Tak	Tak	Tak	Tak	Tak	Tak
	Anomalie aplikacji	Tak	Tak	Tak	Tak	Tak	Tak
Wykrywanie ataków typu DoS	Wykrywanie wg wartości progowych	Tak	Tak	Tak	Tak	Tak	Tak
	Wykrywanie przy wykorzystaniu inteligentnych samouczących profili	Tak	Tak	Tak	Tak	Tak	Tak
	Maksymalna liczba profili ataków typu DoS	5 000	5 000	5 000	300	120	100
Zapobieganie włamaniom	Zatrzymywanie trwających ataków w czasie rzeczywistym	Tak	Tak	Tak	Tak	Tak	Tak
	Eliminacja pakietów/sesji związanych z atakiem	Tak	Tak	Tak	Tak	Tak	Tak
	Zmiana konfiguracji zapory	Tak	Tak	Tak	Tak	Tak	Tak
	Wysyłanie sygnałów resetowania sesji TCP, komunikatów ICMP	Tak	Tak	Tak	Tak	Tak	Tak
	Rejestrowanie pakietów	Tak	Tak	Tak	Tak	Tak	Tak
Ochrona automatyczna i inicjowana przez użytkownika	Tak	Tak	Tak	Tak	Tak	Tak	
Ochrona przed atakami szyfrowanymi	Blokowanie szyfrowanych ataków w czasie rzeczywistym	Tak	Tak	Tak	Tak	Tak	Tak
Zapora wewnętrzna	Blokowanie ruchu niepożądanego i uciążliwego	Tak	Tak	Tak	Tak	Tak	Tak
	Egzekwowanie szczegółowych reguł bezpieczeństwa	Tak	Tak	Tak	Tak	Tak	Tak
Wysoka dostępność	Przełączanie awaryjne z pamięcią stanu	Tak	Tak	Tak	Tak (dla portów Fast Ethernet)	Tak	Tak
Zarządzanie	Interfejs wiersza poleceń (konsola)	Tak	Tak	Tak	Tak	Tak	Tak
	Komunikacja z IntruShield Manager	Bezpieczny kanał	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli	Taka sama dla wszystkich modeli