Test: WatchGuard Firebox M300 s. 54

Bezpieczeństwo środowisk wirtualnych s. 28

3
2016

Miesięcznik informatyków i menedżerów IT

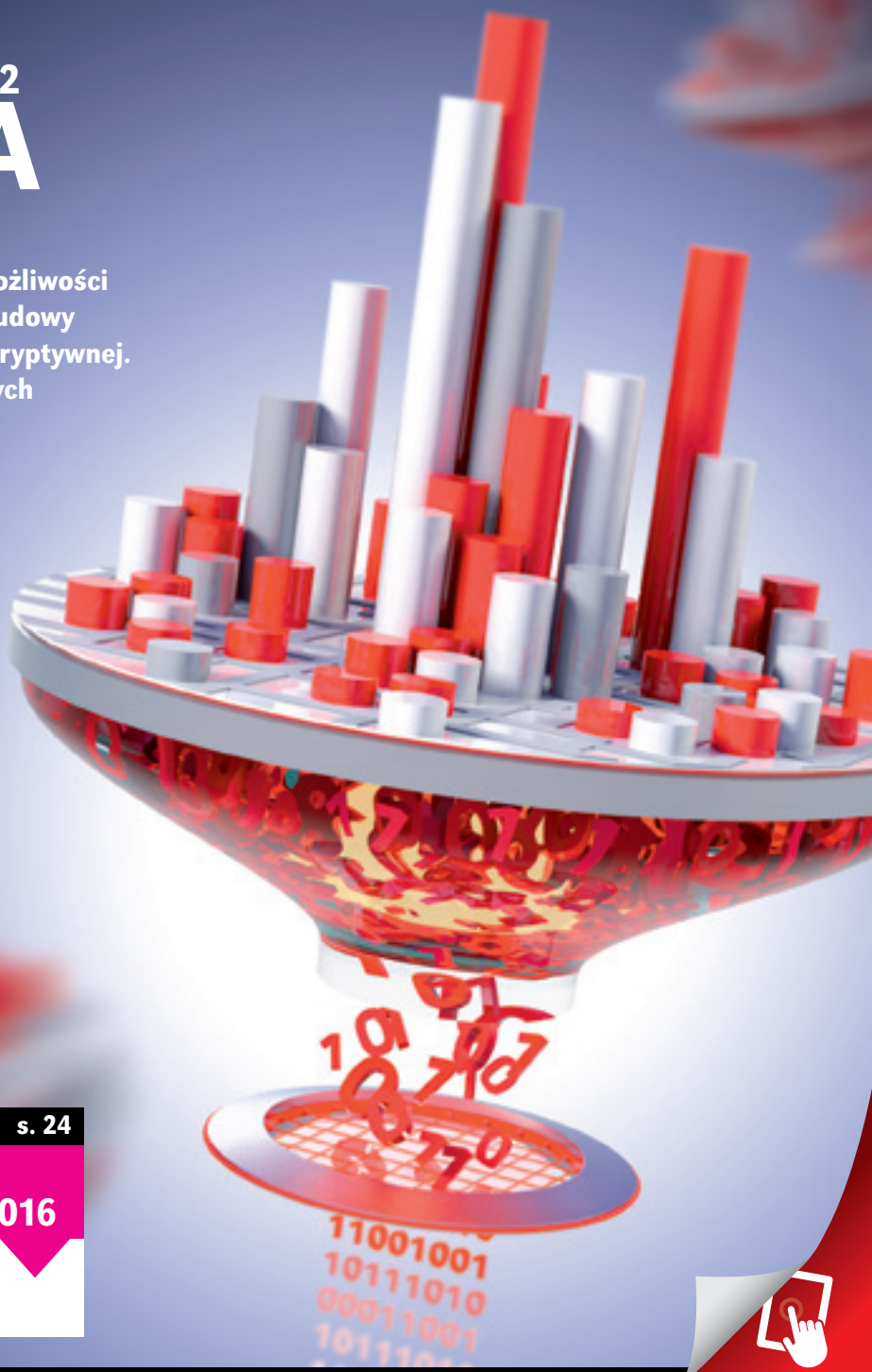
www.it-professional.pl

IT professional

Nr 3 (52) marzec 2016 Cena 33,00 zł (w tym 5% VAT)

ANALIZA BIG DATA s. 12

Wspomaganie procesów decyzyjnych – możliwości pakietu Microsoft Cortana Analytics do budowy zaawansowanych systemów analizy preskryptywnej. Wpływ big data na biznes IT. Analiza danych a przepisy prawa.



ISSN 2083-9588

Serwery ▪ Stacje robocze ▪ Bezpieczeństwo ▪ Infrastruktura i sieci ▪ Zarządzanie i prawo IT ▪ Techn

DOSTĘPNE E-WYDANIE

Zapewnienie bezpieczeństwa na styku sieci lokalnej z internetem to czynność obowiązkowa w każdym przedsiębiorstwie. Pojęcia takie jak Next-Generation Firewall czy Unified Threat Management na dobre zagościły w słowniku administratora. Testujemy wydajne rozwiązanie all-in-one dla MSP.

Urządzenia UTM

WatchGuard Firebox M300

Marcin Jurczyk

Rozwiązania klasy UTM były już niejednokrotnie przedmiotem naszych testów. Tytułem przypomnienia – Unified Threat Management to klasa wielofunkcyjnych produktów chroniących sieć, dedykowanych dla małych i średnich przedsiębiorstw. W tym miejscu należy zaznaczyć, że rynek MŚP w ujęciu globalnym to firmy zatrudniające nawet do 1000 pracowników, co znacznie odbiega od polskich realiów. Wielofunkcyjność rozwiązań UTM to w praktyce konsolidacja wielu mechanizmów ochrony w sieci w formie pojedynczego pudełka realizującego funkcje typu IPS, Next-Generation Firewall, secure Web/Email gateway, antywirus czy kontrola na poziomie aplikacji. Tego typu urządzenia świetnie sprawdzą się w stosunkowo niewielkich firmach, gdzie ochrona zasobów za pośrednictwem rozwiązania all-in-one (często w klastrze HA) uznawana jest za wystarczającą. Tak zwani klienci enterprisowi wymagają znacznie bardziej rozbudowanej ochrony sieci, przy zachowaniu wysokiej wydajności i dostępności na każdym poziomie zabezpieczeń.

WatchGuard Technologies to amerykańska firma z siedzibą w Seattle, działająca na rynku szeroko pojętych zapór ogniowych od 20 lat. Firebox to linia produktów klasy UTM dostępna równolegle z bardziej popularną serią XTM. Portfolio rozwiązań WatchGuard zawiera urządzenia klasy UTM oraz NGFW, a także punkty dostępowe Wi-Fi. Ponadto możliwe jest wdrożenie zabezpieczenia sieci w formie maszyny wirtualnej (XTMv). Warto zauważyć, iż rozwiązania UTM firmy WatchGuard jako jedyne znalazły się w sektorze wizjonerów ostatniego rankingu Gartner Magic Quadrant for Unified Threat Management.

WatchGuard Firebox M300

Specyfikacja
Maks. przepustowość firewalla: 4 Gb/s
Maks. przepustowość VPN: 2 Gb/s
Maks. liczba tuneli IPSec S2S: 75
Maks. liczba tuneli IPSec C2S: 100
Maks. przepustowość SSL VPN: 100
Przepustowość IPS: 2,5 Gb/s
Przepustowość AV: 1,2 Gb/s
Przepustowość UTM: 800 Mb/s
Liczba równoczesnych połączeń: 3,3 mln
Liczba nowych sesji na sekundę: 48 tys.
Liczba interfejsów Gigabit Ethernet: 8

Cena netto
WatchGuard Firebox M300 MSSP Appliance – 1873 euro
WatchGuard Firebox M300, 1 rok Standard Support – 2343 euro
WatchGuard Firebox M300 , 1 rok Security Suite – 3164 euro
WatchGuard WebBlocker 1 rok – 704 euro
WatchGuard Gateway AntiVirus 1 rok – 704 euro
WatchGuard spamBlocker 1 rok – 245 euro
WatchGuard Intrusion Prevention Service 1 rok – 704 euro
WatchGuard Reputation Enabled Defense 1 rok – 704 euro
WatchGuard Application Control 1 rok – 704 euro
WatchGuard Data Loss Prevention 1 rok – 342 euro
WatchGuard APT Blocker 1 rok – 704 euro

> OBUDOWA I WYPOSAŻENIE

Testowany Firebox M300 to przedstawiciel serii dedykowanej średnim przedsiębiorstwom. Urządzenie zamknięto w charakterystycznej czerwonej obudowie 1U. Za komunikację odpowiada osiem miedzianych portów gigabitowych. Na froncie znajduje się ponadto port konsoli (RJ45) oraz dwa porty USB 2.0, a także zestaw diod informujących o stanie pracy urządzenia i przycisk resetu. Do portów USB można podpiąć pamięć zewnętrzną lub modem, który może zostać wykorzystany jako kolejny interfejs do łączenia z internetem. Z tyłu obudowy znajdziemy jedynie gniazdo zasilacza, włącznik oraz kratkę wentylatora. Za wydajność UTM-a odpowiada 4-rdzeniowy (8 wątków) procesor Freescale T2081. Jednostka obliczeniowa to procesor RISC wykonany w architekturze Power. W M300 zainstalowano 4 GB pamięci operacyjnej DDR3L ECC oraz 8 GB kartę microSD, odpowiadającą za przechowywanie danych.

> WYDAJNOŚĆ

WatchGuard na stronie internetowej informuje o bezkonkurencyjnej wydajności Fireboxa M300. Producent powołuje się na wyniki testów przeprowadzonych przez Miercom – niezależną organizację znaną z testów i certyfikacji różnorodnych rozwiązań. Największa przewaga Fireboxa ujawnia się w przypadku, gdy uruchomione zostały równocześnie funkcje zapory ogniowej, IPS, AV, a także kontrola aplikacji. Jak łatwo się domyślić, wraz z uruchomieniem kolejnych mechanizmów kontroli ruchu sieciowego spada wydajność całego urządzenia. W przypadku rozwiązań firmy WatchGuard spadek ten jest jednak najmniejszy w porównaniu z testowanymi UTM-ami konkurencji. Dane katalogowe potwierdzają spore możliwości modelu M300. Przepustowość samej zapory ogniowej określona została na poziomie 4 Gb/s. Dołączenie funkcji IPS powoduje spadek wydajności do 2,5 Gb/s, a modułu antywirusowego do 1,2 Gb/s. W przypadku uruchomienia wszystkich mechanizmów filtracji i bezpieczeństwa, a więc w pełnym trybie UTM, wydajność M300 spada do 800 Mb/s, co w przypadku rozwiązania dedykowanego średnim firmom wciąż stanowi bardzo dobry wynik. Urządzenie obsługuje ponadto do 100 tuneli VPN (IPSec/SSL/L2TP) z maksymalną przepustowością 2 Gb/s. M300 wspiera do 3,3 mln równoczesnych połączeń (dwukierunkowych) oraz do 48 tysięcy nowych połączeń na sekundę. Mówiąc o limitach związanych z modelem M300, należy wspomnieć o 200 wspieranych VLAN-ach i 500 uwierzytelnionych użytkownikach.

Za pośrednictwem reguł firewalla konfiguruje się większość mechanizmów bezpieczeństwa.

> BEZPIECZEŃSTWO

Głównym zadaniem urządzeń UTM jest zapewnienie wszechstronnego bezpieczeństwa na brzegu sieci. Liczba dostępnych modułów bezpieczeństwa, a także sposób ich wykorzystania zależą już tylko od wymagań administratora. W przypadku Fireboxa mamy do czynienia z całą paletą dostępnych mechanizmów. Urządzenia WatchGuard pracują pod kontrolą autorskiego systemu operacyjnego Fireware, który odpowiada za wydajność i współpracę wszystkich modułów bezpieczeństwa. Podstawowa funkcjonalność UTM-a to zapora ogniowa typu stateful packet inspection. W przypadku Fireboxa mamy do czynienia z dwoma sposobami zarządzania ruchem sieciowym – standardowymi regułami filtrowania pakietów IP i nagłówków TCP/UDP oraz filtrowania z wykorzystaniem proxy. W pierwszym przypadku wystarczy dopasowanie na podstawie nagłówka TCP/UDP, aby podjąć odpowiednią akcję. W przypadku zastosowania proxy mamy do czynienia z głęboką inspekcją pakietów, gdyż oprócz danych zawartych w nagłówku analizowana jest również zawartość pakietów pod kątem zagrożeń.

Ten przeznaczony dla średnich przedsiębiorstw UTM po włączeniu kolejnych mechanizmów kontroli ruchu sieciowego jest bezkonkurencyjny pod względem wydajności.

Domyślnie administrator, tworząc kolejne reguły, może wybrać spośród predefiniowanych filtrów oraz ustawień proxy. W przypadku rozwiązań UTM WatchGuard podczas konfiguracji proxy definiuje się większość mechanizmów bezpieczeństwa. Firebox wspiera budowanie zasad proxy dla następujących protokołów: DNS, FTP, H.323, HTTP, HTTPS, POP3, SIP, SMTP oraz TCP-UDP. Z regułami proxy związane są również odpowiednie akcje, będące w praktyce grupą ustawień charakterystycznych dla danego protokołu proxy. Domyślnie dostarczona jest predefiniowana lista akcji dla każdego

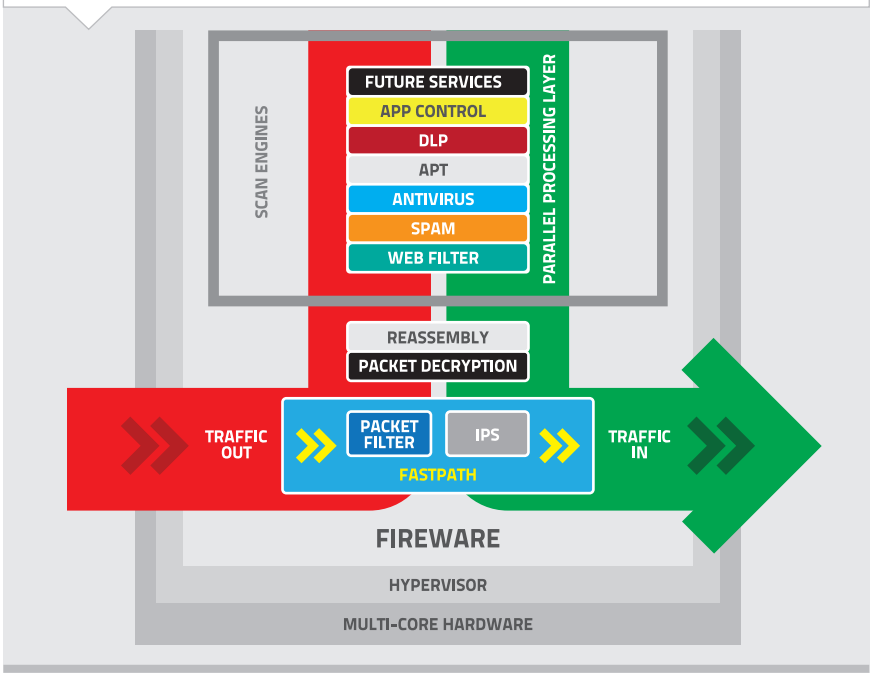
protokołu, którą można rozbudować w zależności od własnych preferencji.

Funkcją standardową dostępną w podstawowej wersji UTM-a jest również koncentrator VPN. Firebox umożliwia zestawienie połączeń typu site-to-site czy client-to-site. W przypadku pierwszej opcji mamy do czynienia z opcją BOVPN (Branch Office VPN), która wykorzystuje protokół IPSec. Mobile VPN z kolei pozwala na zestawienie kanałów z wykorzystaniem IPSec, SSL, PPTP oraz L2TP.

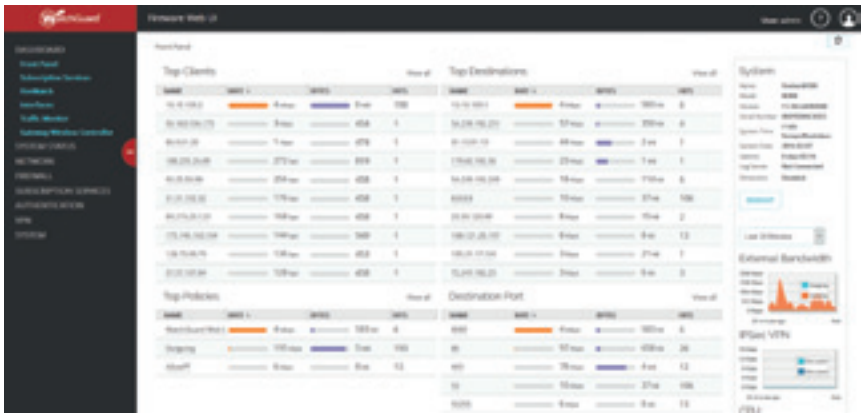
Pozostałe mechanizmy bezpieczeństwa M300 stanowią wyposażenie opcjonalne, dostępne w formie płatnej subskrypcji. W zależności od potrzeb możliwe jest wykupienie dostępu do jednej lub wielu z następujących funkcji zabezpieczeń: IPS, Application Control, WebBlocker, Gateway AntiVirus, spamBlocker, Reputation Enabled Defense, Data Loss Prevention czy APT Blocker.

W przypadku **IPS** mamy do czynienia ze standardowym systemem wykrywania zagrożeń opartych na sygnaturach i zapobiegania im. System ten z powodzeniem zablokuje ataki typu SQL injection, cross-site scripting czy buffer overflow. UTM może pracować w trybie full scan, analizując wszystkie pakiety, a także fast scan, wykorzystującym próbkowanie ruchu, co znacznie podnosi wydajność rozwiązania. Administrator ma oczywiście możliwość pełnej parametryzacji IPS-a w zależności od własnych preferencji.

ARCHITEKTURA SYSTEMU FIREBOX



Kolejny mechanizm dostępny w formie subskrypcji, **Application Control**, umożliwia filtrowanie ruchu na podstawie zestawu zdefiniowanych aplikacji. Identyfikacja ruchu odbywa się na podstawie analizy wzorców pakietów, analizy portów L4, sprawdzania certyfikatów SSL czy korelacji ruchu z sygnaturami. WatchGuard udostępnia sygnatury dla ponad 1800 aplikacji. Sygnatury zostały skategoryzowane, aby ułatwić pracę administratorom. Application Control pozwala łatwo zdefiniować dostęp do najpopularniejszych serwisów i aplikacji, co wykorzystywane jest w domyślnych raportach wykorzystania łącza. Granulacja rozpoznawania poszczególnych aplikacji pozwala na ograniczanie dostępu do wybranych funkcji aplikacji webowych, takich jak pobieranie plików, komunikatory czy gry online. Kontrola aplikacji możliwa jest z dokładnością do pojedynczej reguły firewalla, dla której można określić konkretną akcję Application Control.



Dashboard/Front Panel umożliwia podgląd podstawowych parametrów UTM.

Podobne funkcje realizuje kolejny opcjonalny moduł – **WebBlocker**. Główna różnica polega na tym, że korzysta on z http lub https proxy i ogranicza się do kontroli treści webowych. Wykorzystuje on bazę Websense lub SurfControl, aby na podstawie dostępnych kategorii umożliwić administratorowi łatwe i proste filtrowanie treści. Filtrowanie oparte na proxy wykorzystują wszystkie pozostałe mechanizmy dostępne w modelu subskrypcyjnym. **Gateway AntiVirus** może być wykorzystywany z proxy HTTP, SMTP, POP3, FTP oraz TCP-UDP. W zależności od obsługiwanego protokołu dostępne są zróżnicowane akcje związane z wykryciem zagrożenia.

Moduł potrafi skanować skompresowane załączniki poczty e-mail, pobierane pliki i wiadomości.

Mechanizm kwarantanny umożliwia składowanie podejrzanych obiektów na lokalnym serwerze, podobnie jak w przypadku **spamBlockera**. Ten z kolei potrafi filtrować wiadomości e-mail, korzystając ze wzorców, prostych zasad czy serwerów reputacji. Poza tradycyjnym blokowaniem czy przenoszeniem do kwarantanny popularną akcją jest też tagowanie wiadomości, dzięki któremu odbiorca ma możliwość ich samodzielnego kategoryzowania. **Reputation Enabled Defense** (RED) to z kolei mechanizm wykorzystujący serwer reputacji WatchGuard bazujący na ocenie punktowej adresów URL w zakresie 1–100. Na podstawie wyniku z bazy i lokalnie ustawionego poziomu zagrożenia RED podejmuje decyzje o zezwoleniu na dany ruch, wysłaniu do lokalnego skanera AV czy odrzuceniu ruchu. Dla adresów niezweryfikowanych dotychczas w bazie WatchGuard, które zostały przeskanowane przez lokalny skaner AV lub APT, domyślnie ustawione jest przesyłanie wyniku sprawdzenia na serwer producenta w celu poprawienia skuteczności mechanizmu RED. Wysyłanie tego typu informacji można również wyłączyć.

APT (Advanced Persistent Threat) **Blocker** to kolejny mechanizm bezpieczeństwa odpowiadający za wykrywanie i blokowanie najbardziej zaawansowanych zagrożeń, w tym zagrożeń zero-day, dla których nie opublikowano dotychczas sygnatur IPS czy AV. Dla pobieranych plików i załączników mailowych tworzony jest skrót MD5, który następnie przesyłany jest szyfrowanym kanałem do usługi chmurowej zawierającej bazę danych skrótów. Jeśli wystąpi dopasowanie, możliwe jest natychmiastowe podjęcie odpowiedniej akcji. W przeciwnym przypadku plik przesyłany jest do środowiska testowego (sandbox) gdzie odbywa się analiza zagrożenia w czasie rzeczywistym. W przypadku wykrycia zagrożenia w środowisku sandbox Firebox generuje odpowiednie alerty. APT Blocker potrafi skanować pliki Windows PE, PDF,

Intrusion Prevention System to funkcjonalność, której subskrypcję warto wykupić.

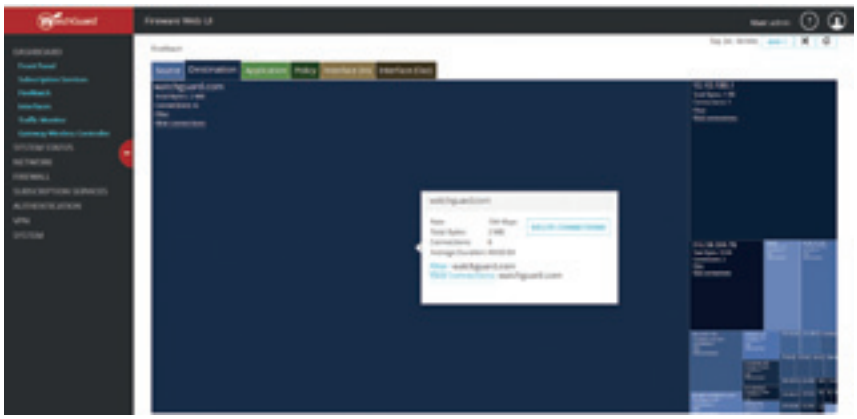
dokumenty MS Office, RTF, aplikacje dla systemu Android (APK), a także skompresowane archiwa gzip, tar i zip. Moduł ten wykorzystuje mechanizm proxy dla protokołów: HTTP, FTP, SMTP i POP3. Funkcja ta wykorzystuje usługi firmy Lastline. Możliwe jest również uruchomienie lokalnej kopii serwera Lastline, do którego przekierowywane będą pliki z APT Blockera.

Ostatnim modułem subskrypcyjnym jest **Data Loss Prevention**, a więc mechanizm umożliwiający wykrycie, monitorowanie i zapobieganie niekontrolowanym wypływom poufnych informacji poza granice sieci wewnętrznej. Wbudowane sensory HIPAA oraz PCI pozwalają na wykrywanie wycieków z wykorzystaniem predefiniowanych zasad. Możliwe jest również tworzenie własnych reguł filtrowania. Sensor potrafi przeskanować tekst zapisany we wszystkich najpopularniejszych formatach. Mechanizm ten współpracuje z regułami proxy dla protokołów HTTP, HTTPS, SMTP i FTP.

Usługodawcami dla opisanych modułów subskrypcyjnych są liderzy w danej branży zabezpieczeń, a więc takie firmy jak Sophos, Websense, Cyren, AVG, Trend Micro czy Lastline, dzięki czemu łatwo zweryfikować skuteczność danego rozwiązania.

> WDROŻENIE I KONFIGURACJA

Podstawowa konfiguracja Fireboxa jest stosunkowo prosta, co charakteryzuje większość urządzeń UTM dostępnych na rynku. Przed podłączeniem urządzenia należy je najpierw aktywować na stronie producenta i dopiero potem można je podpiąć do sieci. Domyślnie pierwszy port (numerowane od 0) prekonfigurowano jako External, co oznacza



Firewatch pozwala na podgląd ruchu sieciowego w czasie rzeczywistym.

Z tyłu obudowy znajdziemy jedynie gniazdo zasilacza, włącznik oraz kratkę wentylatora.

połączenie z niezaufaną, potencjalnie niebezpieczną strefą – internetem. Kolejny port domyślnie ustawiony jest jako Trusted, a więc odpowiada zaufanej, lokalnej sieci LAN. Na porcie tym uruchomiony jest również serwer DHCP. Wystarczy zatem podpiąć do niego komputer, aby połączyć się z webowym interfejsem konfiguracyjnym WebGUI.

W momencie aktywacji użytkownik wybiera sposób konfiguracji urządzenia – RapidDeply QuickStart lub Classic Activation. Pierwsza metoda umożliwia pobranie pliku konfiguracyjnego z prekonfigurowanymi, rekomendowanymi ustawieniami UTM. Klasyczna aktywacja umożliwia z kolei przeprowadzenie wstępnej konfiguracji z wykorzystaniem kreatora. W obu przypadkach Firebox umożliwia inicjowanie połączeń z wewnątrz (TCP, UDP, ICMP) oraz blokuje wszystkie połączenia generowane od strony interfejsu typu External. Kolejnym typem interfejsu jest interfejs Optional, obsługujący mieszaną strefę bezpieczeństwa, odpowiadającą za realizację strefy DMZ. Jeśli z jakiegoś powodu istnieje konieczność wydzielenia dodatkowego rodzaju interfejsu ze względu na strefę bezpieczeństwa, możliwe jest zdefiniowanie interfejsu Custom. Poza przypisaniem typu strefy bezpieczeństwa każdy z interfejsów może być określony jako Bridge, VLAN, Disabled lub Link Aggregation. Z typami interfejsów powiązane są bezpośrednio aliasy wykorzystywane w procesie budowania reguł firewalla (np. Any-Trusted, Any-External).

M300 może zostać wdrożony w jednym z trzech trybów sieciowych: Mixed routing, Drop-in lub Bridge. Pierwszy tryb jest zarazem domyślną opcją i umożliwia wykorzystanie największej ilości dostępnych funkcji bezpieczeństwa. Firebox w trybie Mixed routing pracuje jako standardowa brama na brzegu sieci – każdy z interfejsów musi być skonfigurowany w innej podsieci, urządzenie pracuje jako router (wspierane protokoły routingu dynamicznego: RIP, RIPng, OSPF, OSPFv3 oraz BGP), realizuje translacje adresów NAT itp. Tryb Drop-in, jak nazwa wskazuje, umożliwia wdrożenie bez konieczności modyfikacji ustawień urządzeń pracujących w sieci lokalnej. W tej konfiguracji UTM skonfigurowany jest z pojedynczym adresem IP na wszystkich interfejsach. Logicznie urządzenie w trybie drop-in umieszcza się pomiędzy routerem brzegowym a siecią LAN. Ostatni tryb to klasyczny bridge pomiędzy interfejsami. Jak łatwo się domyślić, tryby drop-in oraz bridge niosą za sobą wiele ograniczeń wynikających ze specyfiki przetwarzania ruchu sieciowego.

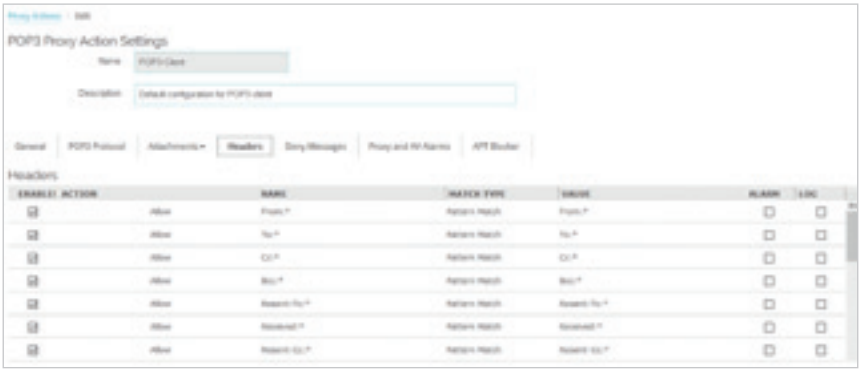
> Trudno wskazać równie wydajny UTM oferujący tak rozbudowane funkcje bezpieczeństwa i wydajność, przy zbliżonym poziomie wydajności.

Jeśli już wybrano odpowiedni tryb pracy, możliwe jest przejście do konfiguracji zabezpieczeń. Większość czynności związanych z konfiguracją zasad bezpieczeństwa odbywa się za pośrednictwem menedżera zasad **WatchGuard System Manager** lub opcji **Firewall Policies** (WebGUI).

Jak już wcześniej wspomniano, większość mechanizmów bezpieczeństwa dostępnych w formie subskrypcji wymaga konfiguracji zasad przy użyciu reguł proxy. Jest to specyficzne podejście do tematu charakterystyczne dla produktów WatchGuard pracujących pod kontrolą systemu Fireware. Skuteczne i efektywne wdrożenie wymaga od administratora dokładnego zapoznania się z dokumentacją, aby zrozumieć ideę działania firewalla bazującego na regułach proxy. Doświadczenie zdobyte podczas pracy z UTM-ami innych producentów może być mało pomocne. Jeśli dodatkowo zamierzamy wykorzystać pełny pakiet możliwości dostępnych za pośrednictwem wszystkich możliwych usług subskrypcyjnych, nie obędzie się bez wnikliwej analizy i testów przedprodukcyjnych.

> ZARZĄDZANIE I MONITORING

Możliwości zarządzania urządzeniami WatchGuard znacznie wykraczają poza standardy obowiązujące na rynku



Większość zaawansowanych mechanizmów bezpieczeństwa wymaga użycia reguł proxy.

PODSUMOWANIE

WatchGuard Firebox M300 to ciekawa propozycja na rynku rozwiązań klasy UTM przeznaczonych dla klientów z sektora MŚP. Nieszablonowe podejście do zagadnień bezpieczeństwa z wykorzystaniem reguł filtrowania bazującego na usługach proxy początkowo może wydawać się skomplikowane. Tym bardziej iż większość zaawansowanych funkcji wykorzystujących opcjonalną subskrypcję wymaga użycia właśnie reguł tego typu. Mnogość mechanizmów bezpieczeństwa, włączając w to skaner antywirusowy, antyspam, kontrolę aplikacji czy funkcję sandboksa w chmurze APT, w połączeniu z imponującą wydajnością w tej klasie rozwiązań sprawiają, że testowany model może okazać się ciekawym wyborem. Przemawia za tym również konkurencyjna cena i przejrzysty model licencjonowania. Trudno wskazać równie wydajny UTM oferujący tak rozbudowane funkcje bezpieczeństwa i wydajność, przy zbliżonym poziomie wydajności. UTM dodatkowo może również pełnić funkcje kontrolera Wi-Fi dla punktów dostępowych WatchGuard. Uniwersalność rozwiązania zasługuje na duży plus. Trzeba jednak pamiętać, że w przypadku wdrożenia tego typu rozwiązań all-in-one konieczne jest szczegółowe zaplanowanie i zdefiniowanie tego, co konkretnie zamierzamy uzyskać jako efekt końcowy.

rozwiązań UTM. Administrator ma do wyboru kilka metod zarządzania – za pośrednictwem interfejsu WebGUI, poprzez interfejs linii komend, a także za pomocą dedykowanego oprogramowania instalowanego na stacji roboczej WatchGuard System Manager. W przypadku administrowania pojedynczym urządzeniem świetnie sprawdzi się WebGUI. Interfejs jest dobrze zaprojektowany, a odnalezienie najbardziej potrzebnych funkcji nie przysparza trudności. Mnogość opcji i ustawień związanych z bezpieczeństwem sprawia, że mimo logicznego układu menu można się w nim łatwo pogubić. Dotyczy to jednak specyficznych ustawień, a po kilku dniach obcowania z WebGUI można nad nim zapanować.

System Manager dużo lepiej sprawdzi się w przypadku zarządzania większą liczbą urządzeń, choć należy przyznać, że konfiguracja i kontrola reguł bezpieczeństwa za pośrednictwem wbudowanego Policy Managera jest znacznie bardziej przejrzysta i intuicyjna. Podczas instalacji System Managera można również zainstalować dodatkowe usługi, takie jak Management Server, Log Server, Report Server, Quarantine Server oraz WebBlocker Server. To właśnie za pośrednictwem Management Servera możliwe jest zarządzanie większą liczbą urządzeń WatchGuard. Zarówno za pośrednictwem interfejsu webowego, jak i WSM możliwy jest podgląd w czasie rzeczywistym działania filtrowania na podstawie zaimplementowanych reguł firewalla Traffic Monitor. Funkcja ta jest szczególnie przydatna w początkowej fazie wdrożenia, kiedy konieczne jest zdefiniowanie odpowiednich zasad. Jedną z opcji możliwych do skonfigurowania tylko za pośrednictwem WSM jest klaster FireCluster. Para dokładnie takich samych urządzeń może zostać skonfigurowana w trybie active-passive lub active-active tylko za pośrednictwem interfejsu System Managera.

WatchGuard standardowo udostępnia też dodatkowe narzędzie o nazwie **Dimension** – do monitoringu, analizy oraz wizualizacji ruchu sieciowego. Narzędzie to dostępne jest w formie predefiniowanej maszyny wirtualnej przeznaczonej na platformę VMware (plik OVA) lub Hyper-V (plik VHD). Dimension to narzędzie analityczne, umożliwiające podgląd logów w czasie rzeczywistym, szczegółowych informacji o ruchu sieciowym przetwarzanych przez urządzenia WatchGuard, a także generowanie raportów na podstawie gromadzonych danych. Narzędzie to składa się z czterech komponentów: Log Collector, Server, Log Database oraz Web Services. Log Collector odpowiada za zbieranie logów z urządzeń Firebox, klastrów Fire Cluster oraz serwerów WatchGuard, a także ich agregację w formie podsumowań i raportów. Server realizuje funkcje API dla danych z logów oraz zapewnia utrzymanie usługi Dimension. Web Services dostarczają interfejs webowy użytkownikom i administratorom, a Log Database realizuje przechowywanie danych. To scentralizowane narzędzie pozwala uzyskać szybki wgląd we wszystkie aspekty działania rozproszonej sieci urządzeń WatchGuard UTM. IT

Autor jest architektem w międzynarodowej firmie z branży IT. Zajmuje się infrastrukturą sieciowo-serwerową, wirtualizacją infrastruktury i pamięcią masową.

Werdykt

WatchGuard Firebox M300

Zalety

- ⊕ wysoka wydajność w tej klasie urządzeń
- ⊕ rozbudowane mechanizmy kontroli ruchu
- ⊕ zróżnicowane możliwości zarządzania
- ⊕ aplikacja Dimension
- ⊕ stosunek cena/jakość
- ⊕ proste licencjonowanie

Wady

- ⊖ konfiguracja zaawansowanych mechanizmów bezpieczeństwa poprzez reguły proxy może wydawać się skomplikowana

Ocena **8**/10