UTM I FIREWALL

WYBÓR CZYTELNIKÓW:

Fortinet FortiGate 300C

W FortiGate 300C zintegrowano zestaw niezbędnych funkcji zapewniających bezpieczeństwo zarówno aplikacjom, jak i danym. Umieszczono tu mechanizmy przeciwdziałające zaawansowanym zagrożeniom od strony sieci publicznej oraz propagującym się przez zainfekowane hosty z sieci wewnętrznej. Technika Global Threat Research Team Fortinet i silniki certyfikowane przez ICSA Labs zapewniają wysoki poziom usług zabezpieczających. UTM pełni funkcję firewalla, IPS-a, serwera VPN, antywirusa, antyspamera oraz filtra stron WWW z zaawansowaną kontrolą treści. Funkcjonalność DLP, czyli Data Leak Prevention, pozwala dodatkowo na kontrolowanie i blokowanie prób przesyłania danych na podstawie zdefiniowanych sygnatur w urządzeniu. Nagrodzone urządzenie oferuje wiele opcji integracji z zewnętrznymi serwerami: od LDAP, poprzez RADIUS i TACACS+ po Directory Service. Uruchamiając integrację z Active Directory, możemy uzależnić naszą politykę bezpieczeństwa od już istniejących obiektów użytkowników i grup, co daje możliwość stosowania zasad z dokładnością do grup. Reguły firewalla mogą być kojarzone nie tylko z ruchem pakietowym typu od, do i gdzie, ale także korzystać z profili ochrony IPS, antywirusa, e-mail czy DLP. FortiGate 300C pozwala na tworzenie wirtualnych domen (VDOM). Pozwalają one na separację stref, użytkowników, polityk firewalla, routingu oraz konfiguracji VPN. Każda z osobnych konfiguracji jest wirtualnym systemem, znajdującym się w jednym fizycznym urządzeniu. Pozwala to logicznie podzielić ustawienia na grupy robocze, a także ułatwia konfigurację w przypadku skomplikowanych zestawów reguł i profili poszczególnych modułów. VDOM jest ułatwieniem dla administratorów zarządzających skomplikowanymi konfiguracjami w sieciach segmentowanych na grupy robocze pracujące w wirtualnych sieciach.

Opinia Czytelników:
Używamy tego sprzętu w pracy, to jedno z najlepszych rozwiązań do kontroli treści, ograniczające dostęp i nadzorujące działania użytkowników w internecie.

TOP 10
(wybór Czytelników)

01. Fortinet FortiGate 300C
02. Cisco ASA5520
03. Netasq U250
04. Check Point 61000 Security System
05. DrayTek Vigor 2110Vn
06. Check Point 21400 Appliance
07. D-Link UTM DFL-260
08. Barracuda Spam&Virus Firewall
09. Netasq U70 gateProtect GPZ 5000
10. Symantec Brightmail

WYBÓR REDAKCJI:

Check Point 21400

Zwycięzca jest superwydajnym UTM-em pozwalającym filtrować pakiety przy wsparciu sprzętowym z wydajnością do 110 Gbps (w przypadku firewalla) oraz do 21 Gbps (w przypadku analizatora IPS). Urządzenie korzysta z technologii Check Point 3D, będącej kombinacją różnych metod zabezpieczających: firewall, VPN, IPS, Application Control, Mobile Access, DLP, URL Filtering, Antivirus, Anti-spam, Anti-Bot, Identity Awareness oraz Advanced Networking & Clustering. Firma Check Point wprowadziła miarę SecurityPower, rzeczywistej wydajności swoich urządzeń, która ma odzwierciedlać faktyczną prędkość rozwiązania w środowisku produkcyjnym. Sprzęt o oznaczeniu 21400 otrzymał 2900 jednostek SecurityPower, co pozwala dedykować go dużym organizacjom oraz centrom danych. Check Point 21400 może być wyposażony w 36 miedzianych portów GE lub 10 światłowodowych portów GE. Sprzęt jest modularny, posiada redundantne zasilanie i macierz RAID. Dyski oraz zasilacze można wymieniać na gorąco (hot-swap) w trakcie pracy. Dostępny jest też opcjonalny moduł przyspieszający działanie urządzenia, dzięki któremu prędkość analizy pakietów przeprowadzanych przez moduł firewall wzrasta z 50 Gbps do 110 Gbps i maks. 5 µs opóźnienia. Maksymalna ilość połączeń ze wspomnianym modułem wynosi 300 000 na sekundę.

Uzasadnienie:
Check Point w wersji 21400 cechuje się wysoką wydajnością, skalowalnością oraz niezawodnością. Zastosowane technologie gwarantują osiągnięcie wysokiego poziomu bezpieczeństwa w sieciach korporacyjnych oraz centrach danych.