IT w administracji
Miesięcznik informatyków i menedżerów IT sektora publicznego

nr 7–8 (200–201) lipiec–sierpień 2024 | itwadministracji.pl

Konteneryzacja

Efektywne wykorzystanie zasobów systemowych w urzędzie

DOSTĘPNE E-WYDANIE

ISSN 1898-3227
cena 82,00 zł (w tym 8% VAT)
9 771898 322000

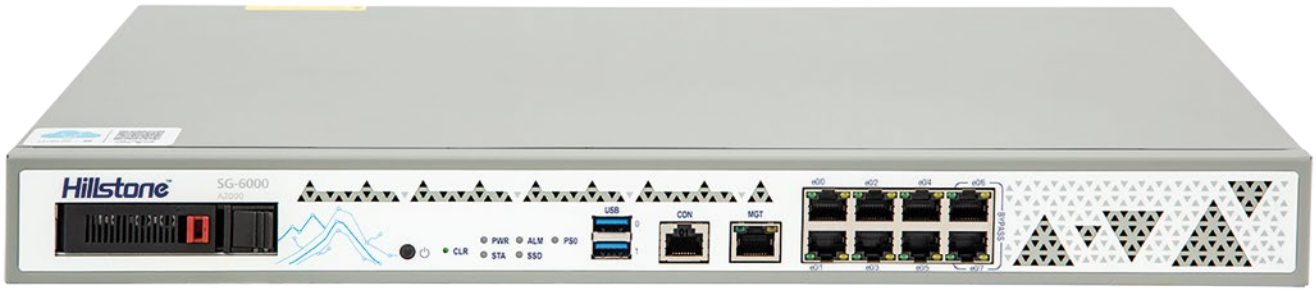
FIREWALLE NGFW HILLSTONE SG-6000 A2000

Ochrona przed cyberatakami

Z roku na rok wzrasta liczba przeprowadzanych cyberataków, dlatego temat bezpieczeństwa danych nie powinien być obojętny jednostkom administracji publicznej. Jednym z najlepszych sposobów na podniesienie poziomu ochrony jest instalacja sprzętowego firewalla.

Marek Budny

W ostatnich latach wiele usług realizowanych przez administrację publiczną zostało przeniesionych do sfery cyfrowej. Coraz więcej spraw urzędowych możemy załatwić online, nie wychodząc z domu i korzystając jedynie z komputera z dostępem do internetu. W związku z tym rośnie odpowiedzialność instytucji za bezpieczeństwo gromadzonych i przechowywanych danych. Mimo stosowania różnych systemów bezpieczeństwa, regulaminów i procedur ważne staje się także właściwe zabezpieczenie styku sieci lokalnej z internetem przed cyberatakami z zewnątrz. Urządzeniami, które do tego służą, są sprzętowe firewalle. Jednym z nich jest Hillstone SG-6000 A2000. To urządzenie klasy NGFW (Next-Generation Firewall), zaprojektowane dla średniej wielkości organizacji (od 75 do 150 stacji roboczych).



Instalacja i uruchomienie

Dostarczony nam do testu model jest zamknięty w solidnej, metalowej obudowie rackowej o wysokości 1U. Przeznaczono go tym samym do montażu w szafie teleinformatycznej. Zasilanie doprowadza się komputerowym kablem VDE z sieci 230 V. Po włączeniu firewalla komputer z odpowiednio skonfigurowaną kartą sieciową należy podłączyć do gniazda oznaczonego symbolem MGT i przejść do panelu administratora, który można uruchomić w przeglądarce internetowej. Jest on częścią systemu operacyjnego StoneOS, opracowanego przez firmę Hillstone do stosowania w urządzeniach NGFW. Podczas pierwszego logowania można zmienić domyślne hasło na wybrane przez siebie. Oprócz graficznego interfejsu użytkownika (GUI) do zarządzania zaporą SG-6000 A2000 jest dostępny także interfejs wiersza poleceń (CLI – Command Line Interface), realizowany przez bezpieczną powłokę Secure Shell – SSH. W urządzeniu zamontowano ponadto gniazdo konsoli CON, które również można wykorzystać do konfiguracji zapory z wykorzystaniem interfejsu szeregowego RJ-45 na USB lub RS-232.

Po wejściu w tryb konfiguracji urządzenia należy kolejno zainstalować licencje zakupionych usług i modułów bezpieczeństwa, podłączyć zaporę do internetu, ustawić serwer DNS i przekierować ruch z bramy sieciowej na wybrany interfejs. Model A2000 wyposażono w osiem gigabitowych portów RJ-45, które można wykorzystać do obsługi sieci LAN i podłączenia firewalla do sieci WAN.

Do pełnego uruchomienia firewalla potrzebne jest jeszcze wyznaczenie stref bezpieczeństwa porządkujących w firewallu zasady ochrony, zwane też politykami. Polityka bezpieczeństwa umożliwia obustronny ruch sieciowy między siecią globalną a lokalną. A2000 wyposażono w predefiniowane strefy bezpieczeństwa (Network/Zone), które można wykorzystać w podstawowym zakresie w prostych lub tymczasowych zastosowaniach. Do szczegółowego administrowania bezpieczeństwem konieczne jest jednak stworzenie własnych stref i polityk do obsługi konkretnych potrzeb.

Konfiguracja polityk bezpieczeństwa

Administrator konfigurujący Hillstone SG-6000 A2000 ma do dyspozycji wiele opcji i parametrów. Definiując politykę bezpieczeństwa w zakładce ustawień, warto przyjrzeć się trzem sekcjom – Threat Protection, Data Security i Options – w których znajdują się kluczowe ustawienia parametrów pracy firewalla. (Dwie pierwsze są także dostępne podczas definiowania stref bezpieczeństwa). W kategorii Threat Protection ustawiamy ochronę antywirusową,

Hillstone SG-6000 A2000

Przepustowość firewalla: 5 Gb/s
Przepustowość NGFW: 1,2 Gb/s
Przepustowość antywirusa: 2 Gb/s
Przepustowość Threat Protection: 800 Mb/s
Przepustowość IPS: 3,2 Gb/s
Przepustowość IPSec VPN: 2700 Mb/s
Maksymalna liczba sesji jednoczesnych: 1 mln
Liczba polityk firewalla: 8000
Liczba użytkowników SSL VPN: 1000
Liczba tuneli IPSec: 4000
Porty zarządzania: Console Port RJ-45, 2 × USB 3.0, MGT Port RJ-45
Porty I/O: 8 × Gigabit Ethernet (w tym 1 para bypass)
Pamięć wbudowana: 8 GB
Możliwość rozbudowy pamięci: dysk SSD 500 GB / 1 TB / 2 TB
Zasilanie: AC 100–240 V 50/60 Hz
Pobór mocy: 50 W
Typ obudowy: rack 1U
Wymiary (szer. × wys. × gł.): 436 × 44 × 320 mm
Ciężar: 3,9 kg
Zakres temperatur: 0–40˚C
Cena (netto): 9600 zł

jeden z głównych modułów bezpieczeństwa zapory ogniowej Hillstone. Antywirus ma własną, na bieżąco aktualizowaną bazę z sygnaturami wirusów. Konfigurując ochronę przed malware'em można wybrać profil przygotowany przez producenta sprzętu lub zdefiniować własny. Podobnie w sekcji ustawień systemu zapobiegania włamaniom IPS (Instrusion Prevention System) – tam również da się wybrać profil predefiniowany lub własny, a także samodzielnie aktualizować bazę sygnatur. Testowany firewall ma też wbudowany system antyspamowy, zwiększający bezpieczeństwo podczas korzystania z poczty elektronicznej. Administrator może ręcznie dodawać adresy e-mail niechcianych nadawców, a nawet całe domeny.

W sekcji Threat Protection znajdują się jeszcze opcje Botnet Prevention (moduł chroniący przed zagrożeniami pochodzącymi z sieci typu BotNet), Attack Defense (zestaw funkcji do obrony przed atakami), Sandbox (opcja kierowania plików do sprawdzenia pod kątem zagrożeń w izolowanym środowisku) oraz URL Filtering. Ostatnia z wymienionych funkcji blokuje dostęp do podejrzanych stron WWW, opierając się na aktualizowanej bazie reputacji witryn. Administrator może także blokować dostęp ręcznie, tworząc tzw. Black List, ograniczyć możliwość otwierania wybranych stron (np. mediów społecznościowych) w konkretnym przedziale czasowym lub uniemożliwić przejście do serwisów WWW zawierających w nazwie domeny określone słowa.

W zakładce ustawień Data Security do dyspozycji mamy opcje Web Content i Web Posting. Ta pierwsza służy do kontrolowania odwiedzin serwisów WWW na podstawie zdefiniowanej grupy słów kluczowych. Jeśli użytkownik wejdzie na stronę zawierającą w nazwie słowo kluczowe, może to skutkować zablokowaniem dostępu do witryny lub wpisem w dzienników logów. Dzięki temu administrator może prześledzić zachowania użytkowników i jeśli stwierdzi, że są one niebezpieczne dla organizacji – podjąć działania zapobiegawcze. Druga z funkcji – Web Posting – działa na tej samej zasadzie, ale w odwrotnym kierunku: blokuje użytkownikowi możliwość publikowania treści zawierającej słowo kluczowe lub odnotowuje taką aktywność w logach.

W Data Security dostępny jest jeszcze moduł filtrowania wiadomości e-mail (Email Filter). Ustalając odpowiednie reguły, administrator może zablokować pocztę pochodzącą z wybranych adresów e-mail lub zawierającą w treści słowa kluczowe. Zdefiniowany profil filtrowania poczty można następnie podłączyć do polityki bezpieczeństwa firewalla. Ostatnie dwie opcje w Data Security to APP Behavior Control (kontrola działań aplikacji używających protokołów FTP, HTTP i TELNET) i Network Behavior Control (kontrola zachowania w sieci lokalnej).

Monitorowanie ruchu i zagrożeń

Po skonfigurowaniu A2000 mogliśmy w praktyce przetestować, jak urządzenia radzi sobie podczas aktywnej pracy. Cennych informacji o ruchu sieciowym dostarcza znajdująca się w panelu administratora zakładka Monitor. W sekcji User Monitor znajdziemy informację, jaki ruch sieciowy generowali poszczególni użytkownicy w czasie rzeczywistym w ciągu ostatnich 60 minut, 24 godzin lub 30 dni. Sprawdzimy też, którzy pracownicy generują największy ruch sieciowy (10 najbardziej aktywnych). Zakładka Application Monitor gromadzi z kolei dane →

Intel QuickAssist Technology

Firewalle Hillstone Networks z serii A wyposażone są w układ Intel QuickAssist Technology (QAT), którego zadaniem jest odciążenie CPU urządzenia podczas przeprowadzania inspekcji SSL/TLS. Włączenie tej funkcji w innych zaporach ogniowych może doprowadzić do spadku wydajności sięgającej 95-97% przepustowości całego systemu bezpieczeństwa. Benefity płynące z technologii Intel QAT:

- Poprawiona wydajność i efektywność procesora – Intel QAT odciąża rdzenie procesora od operacji kompresji i dekompresji, dzięki czemu poprawia się wydajność CPU, który może w tym czasie realizować inne zadania, zapewniając lepsze działanie systemu.
- Zwiększona wydajność wirtualnych sieci prywatnych (VPN) – technologia Intel QAT przyspiesza szyfrowanie i deszyfrowanie ruchu sieciowego. Może to poprawić wydajność wirtualnych sieci prywatnych, modułów równoważenia obciążenia sieci, dostarczania treści i serwerów WWW przy jednoczesnym wykorzystaniu mniejszej liczby rdzeni niż bez technologii Intel QAT.
- Redukcja poboru mocy – Intel QAT pomaga zmniejszyć koszt eksploatacji poprzez przyspieszenie szyfrowania i odszyfrowywania danych. Do osiągnięcia tego samego rezultatu obliczeniowego potrzeba mniej rdzeni procesora, co prowadzi do mniejszego zużycia baterii.

dotyczące aktywności poszczególnych aplikacji z podziałem na podobne sekwencje czasowe jak w części User Monitor. Na wykresach słupkowych możemy zobaczyć 10 aplikacji generujących najbardziej ryzykowny ruch sieciowy i największy ruch sieciowy w ogóle (z podziałem na kategorie, subkategorie i użyte technologie).

Cechą wyróżniającą firewall A2000 jest rozbudowany system logów, który podzielono na aż 13 kategorii. Urządzenie zapisuje w pamięci zdarzenia o ośmiu poziomach złośliwości (debugging, information, notification, warning, error, critical, alert, emergency). Tworzone są także dzienniki o usługach sieciowych, chronologiczny zapis zagrożeń (Threat Log), logi translacji adresów sieciowych, działania filtru zawartości sieci i jeszcze kilka innych.

Do monitorowania bieżących zagrożeń służy zakładka iCenter w panelu administratora. Jest ona podzielona na dwie sekcje – Threat i Hot Intelligence Monitor. Pierwsza z nich zawiera statystyki i informacje o wszystkich zagrożeniach pochodzących z internetu w określonych przedziałach czasowych. Druga zaś prezentuje, czy zapora ogniowa jest odporna na największe i aktualne zagrożenia internetowe (wirusy, malware, podatność na włamania itp.). Lista wyświetlana jest na ekranie i każda niebezpieczna pozycja oznaczona jest napisem Unprotected na czerwonym tle. Zadaniem osoby zarządzającej firewallem jest doprowadzenie do stanu, w którym lista zagrożeń zostanie oznaczona tekstem Protected na zielonym tle. Sygnalizuje to, że sieć jest chroniona. Można to osiągnąć, podejmując takie działania ochronne jak aktualizacja sygnatur antywirusów, IPS, prewencja zagrożeń z sieci BotNet oraz wdrożenie skutecznych polityk bezpieczeństwa.

Rozbudowana administracja

Zaletą A2000 jest na pewno rozbudowany panel administracyjny. Wśród mnogości funkcji i ustawień warto przyjrzeć się sekcji zarządzania dostępem do urządzenia. Można w niej dodać kolejnych użytkowników uprawnionych do logowania się do A2000. Ich kontom da się przypisać jeden z czterech predefiniowanych poziomów uprawnień: Administrator, Operator, Auditor i Administrator Read-Only. Istnieje również opcja samodzielnego ustawienia praw dla poszczególnych użytkowników, w tym włączenia lub wyłączenia dostępu do konsoli poleceń lub wybranych zakładek interfejsu graficznego (GUI). Pozwala to rozdzielić obowiązki dbania o bezpieczeństwo systemu sieciowego na kilka osób. Aby dodatkowo zwiększyć bezpieczeństwo i ochronę przed niepowołanym dostępem do firewalla, można ustalić jeden adres lub zakres adresów IP uprawnionych do logowania się do urządzenia. Weryfikacja może też polegać na sprawdzeniu adresu MAC. IT

StoneOS 5.5R10 – ulepszona ochrona

System StoneOS używa technologii ZTNA (Zero Trust Network Access) i wykorzystuje uczenie maszynowe do wykrywania zagrożeń podczas szyfrowanej transmisji bez konieczności jej dekodowania. W nowej wersji rozbudowano opcje inteligentnej ochrony przed DDoS, wykrywanie DGA (algorytmy generacji domeny wykorzystywane przez złośliwe oprogramowanie), a także rozszerzono czarną listę IP, co umożliwia lepsze filtrowanie ruchu obwodowego (PTF). Aktualizacja wzbogaciła też funkcje VPN o obsługę ECMP (Equal Cost Multi Path, strategia routingu warstwy 3) i przełączanie awaryjne, co poprawia wydajność połączenia i skuteczność ustanawiania tunelu IPSec VPN.

Autor jest niezależnym dziennikarzem publikującym w magazynach komputerowych. Ma zawodowe doświadczenie w testowaniu sprzętu i oprogramowania komputerowego.

Podsumowanie

Hillstone SG-6000 A2000 to jeden z kilku przedstawicieli rodziny firewallów NGFW. W serii SG-6000 producent oferuje osiem różnych modeli (A1000, A1100, A2000, A2600, A3000, A3600, A3700, A3800), które różnią się między sobą przepustowością i liczbą portów. Dzięki temu możemy wybrać wersję odpowiednią do potrzeb organizacji.

A2000 jest firewallem nowej generacji, charakteryzującym się wysoką wydajnością zabezpieczeń, opcjami rozbudowy oraz bardzo dobrym wykrywaniem zagrożeń i zapobieganiem zaawansowanym niebezpieczeństwom pochodzącym z internetu. Zastosowana nowa architektura sprzętowa zapewnia świetną wydajność warstwy aplikacji, a zaawansowane zabezpieczenia przed znanymi i nieznanymi zagrożeniami w połączeniu z inteligentną i zautomatyzowaną obsługą zasad ochrony przed cyberatakami zapewnią spokojny sen osobom odpowiedzialnym za bezpieczeństwo systemów sieciowych.

Ocena 10/10

Plusy

- pomoc techniczna w języku polskim na stronie WWW dystrybutora
- wsparcie sprzętowe dla akceleracji VPN, SSL-TLS Intel QAT
- kieszeń na dysk twardy (maks. 2 TB) do przechowywania większej ilości logów
- niewielki spadek wydajności w przypadku włączenia wszystkich systemów bezpieczeństwa

Minusy

- kieszeń na dysk SSD jest przystosowana tylko do montażu modułów 2,5 cala