Hillstone Seria A

Inteligentny Firewall Nowej Generacji

Firewall Nowej Generacji Hillstone Serii A zapewnia wysoką wydajność w zakresie bezpieczeństwa, możliwość rozbudowy w razie potrzeby, kompletne zaawansowane wykrywanie zagrożeń, zapobieganie im oraz inteligentne i zautomatyzowane działanie polityk. Seria A NGFW oparta jest na zupełnie nowej architekturze sprzętowej, która oferuje wiodącą w branży wydajność w warstwie aplikacji, aby sprostać rzeczywistym wymaganiom bezpieczeństwa sieci. Porty o dużej gęstości zapewniają doskonałe możliwości dostępu, a wiele opcji pamięci masowej zapewnia lepszą widoczność i analitykę. NGFW Hillstone Serii A oferuje kompletną, zaawansowaną ochronę przed znanymi i nieznanymi zagrożeniami. W połączeniu z inteligentną, zautomatyzowaną i wydajną obsługą polityk sprawia, że operacje bezpieczeństwa są niezwykle łatwe.

Najważniejsze informacje o produktach

Zaawansowane Wykrywanie Zagrożeń i Ochrona

NGFW Hillstone Serii A zawiera pełen arsenał mechanizmów zapewniających wykrywanie i ochronę w czasie rzeczywistym przez cały cykl życia ataków sieciowych i złośliwego oprogramowania. Proaktywne zabezpieczenia, takie jak IPS, blokują wykorzystane luki w zabezpieczeniach zanim dojdzie do naruszenia. Usługi reputacji adresów IP blokują żądania z ryzykownych domen, które mogą zawierać złośliwe oprogramowanie i spam. Filtrowanie adresów URL zapobiega nieumyślnemu dostępowi użytkowników do witryn związanych z phishingiem, pobieraniem złośliwego oprogramowania i innych exploitów. Antywirus wykrywa i blokuje znane złośliwe oprogramowanie na poziomie sieci, dzięki zaawansowanej bazie stale aktualizowanych sygnatur. Antyspam zapewnia klasyfikację spamu w czasie rzeczywistym i chroni zarówno ruch przychodzący i wychodzący.

Podczas włamań Antywirus odgrywa również ważną rolę poprzez bezustanne wykrywanie i blokowanie znanego złośliwego oprogramowanie. Cloud Sandbox zapewnia zaawansowane wykrywanie i zapobieganie złośliwych plików wykorzystując statyczną analizę i przetwarzanie wstępne. Następnie stosuje analizę behawioralną obejmującą wykrywanie technik ukrywania się i omijania. Inteligencja Zagrożeń w Chmurze identyfikuje i blokuje złośliwe pliki, generuje logi i raporty oraz dzieli się inteligencją o zagrożeniach z powrotem do chmury, dzięki czemu wszystkie rozwiązania posiadają aktualne informacje o zagrożeniach.

Uzupełniając stos zabezpieczeń w całym cyklu życia zagrożenia, Seria A kontynuuje ochronę nawet po wystąpieniu naruszenia. Zaawansowana funkcja zapobiegania Botnet C&C firmy Hillstone uniemożliwia komunikację z kanałem sterowania, a także wykrywa i blokuje boty w intranecie.

Najważniejsze informacje o produktach (Ciąg dalszy)

Ponadto ujednolicony mechanizm wykrywania i silniki analityczne koordynują wszystkie wbudowane mechanizmy bezpieczeństwa, aby radykalnie zwiększyć wydajność przy jednoczesnym zmniejszeniu opóźnień w sieci.

Architektura Sprzętowa Wysokiej Wydajności

Architektura sprzętowa o wysokiej wydajności Serii A przygotowana jest na przyszłość. W kompaktowej obudowie umieszczona jest potężna podstawa obliczeniowa, która zapewnia wysoką wydajność i bezkompromisowe bezpieczeństwo. NGFW Serii A oferują solidną wydajność w zakresie przepustowości firewall, jednoczesnych i nowych sesji, a także niesamowicie szybką wydajność w warstwie aplikacji, która ma kluczowe znaczenie w celu spełnienia potrzeb obecnych środowisk bezpieczeństwa. Oferuje również przyjazną ekologię oprogramowania umożliwiając integrację z innymi firmami, aby w razie potrzeby wspierać dodatkowe funkcje bezpieczeństwa. Wszystkie modele przystosowane są do montażu w szafie rack. Posiadają wentylację z przodu i z tyłu, która pomaga w rozpraszaniu ciepła, rozwiązując problemy, które pojawiają się w sieciach o niemal każdej wielkości.

Doskonałe Możliwości Dostępu i Rozszerzenie Pojemności Przechowywania

Seria A Hillstone oferuje wysoką gęstość portów we/wy, umożliwiając NGFW działanie w razie potrzeby jako przełącznik lub router przy jednoczesnym obniżeniu kosztów wdrażania i zarządzania. Ponadto dla wielu modeli z serii A dostępne są sloty rozszerzeń w celu dalszego zwiększenia wydajności. Pary portów bypass większości modeli z Serii A zapewniają ciągłość biznesową.
Wszystkie modele, w tym wersje typu desktop, zawierają dużą wbudowaną pamięć masową o pojemności 8 GB i opcje rozszerzenia do bardzo dużej pojemności na dysku twardym sięgającą 2 TB. Zwiększona pojemność dysku pozwala zapisać więcej logów i danych przez dłuższy czas, umożliwiając przy tym głębszą analizę. Ponadto rozszerzona pamięć umożliwia systemowi dostarczanie bogatszych raportów zawierających znacznie więcej informacji, w tym zwizualizowanych wyników i rekomendowanych działań.

Ponadto, dzięki głębszej analizie zagrożeń, WebUI może wyświetlać znacznie bogatsze informacje o wykrywaniu zagrożeń, co z kolei zapewnia administratorom lepszą widoczność. Zwiększona widoczność pozwala administratorom szybko skupić się na anomaliach i innych podejrzanych zdarzeniach sieciowych lub ruchu oraz analizować i reagować z większą precyzją.

Inteligentne Działanie Polityk (Smart Policy)

Seria A zawiera inteligentne zarządzanie i działanie w całym cyklu życia polityki, od wdrożenia po zarządzanie, optymalizację i eksploatację. System oferuje automatyczne wdrażanie polityk użytkowników przy użyciu dynamicznej autoryzacji RADIUS. Zarządzanie politykami jest znacznie bardziej wydajne dzięki grupowaniu ich na podstawie wymagań biznesowych. Ponadto polityki mogą być agregowane, aby połączyć je tak jakby działały jak pojedyncza polityka. Innowacyjny asystent polityk analizuje wzorce ruchu i zaleca ulepszanie polityk w celu szybszego, łatwiejszego i dokładniejszego zarządzania politykami. Działanie polityk jest bardziej wydajne i precyzyjne dzięki kontrolom nadmiarowości, które identyfikują zbędne polityki, dezaktywują je lub usuwają oraz analizie liczby trafień polityki, która pomaga w dalszym udoskonalaniu i doprecyzowaniu polityk.

Funkcje

Usługi sieciowe

- Routing dynamiczny (OSPF, BGP, RIPv2)
- Routing statyczny i policy routing
- Routing kontrolowany przez aplikacje
- Wbudowane serwery DHCP, NTP, DNS i DNS proxy
- Tryb Tap – łączy się do SPAN portu
- Tryby interfejsu: sniffer, agregowane portów, loopback, VLANy (802.1Q i Trunking)
- L2/L3 routing i switching
- Multicast(PIM-SSM)
- Virtual wire (warstwa L1) wdrożenie przezroczyste inline (transparent inline)

Firewall

- Tryby pracy: NAT/ routing, przezroczysty (mostek) i tryb mieszany
- Obiekty polityk: wstępnie zdefiniowane, niestandardowe, agregacja polityk, grupowanie obiektów
- Polityki bezpieczeństwa oparte na aplikacji, roli i geo-lokalizacji
- Bramy Poziomu Aplikacji i obsługa sesji: MSRCP, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, dcerpc, dns-tcp, dns-udp,H.245 0, H.245 1, H.323
- Obsługa NAT i ALG: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN
- Konfiguracja NAT: per polityka lub centralna tablica NAT
- VoIP: SIP/H.323/SCCP NAT traversal, RTP ping holing
- Widok globalnego zarządzania politykami
- Inspekcja nadmiarowości polityk bezpieczeństwa, grupowanie polityk, wycofywanie konfiguracji polityk (rollback), agregowanie polityk
- Asystent Polityk dla ułatwienia szczegółowego wdrażania polityk
- Analiza polityk i czyszczenie nieprawidłowych polityk
- Kompleksowe polityki DNS
- Harmonogramy: jednorazowe i cykliczne
- Wsparcie importu i eksportu polityk

Zapobieganie włamaniom

- Wykrywanie anomalii protokołów, wykrywanie oparte na ocenie, niestandardowe sygnatury, ręczne, automatyczne wypychanie lub ściąganie aktualizacji sygnatur, zintegrowana encyklopedia zagrożeń
- Akcje IPS: domyślne, monitorowanie, blokowanie, resetowanie (atakujący adres IP lub adres IP ofiary, interfejs przychodzący) z czasem wygaśnięcia
- Opcja logowania pakietów
- Filtr oparty na wyborze: ważność, cel, system operacyjny, aplikacja lub protokół
- Zwolnienie IP ze wybranych sygnatur IPS
- Tryb sniffera IDS
- Ochrona DoS oparta na ocenie IPv4 i IPv6 z ustawieniami progowymi przed TCP Syn flood, skanowaniem portów TCP/ UDP/SCTP, ICMP sweep, TCP/UDP/ SCIP/ICMP flooding sesji (źródło/cel)
- Aktywny bypass z interfejsami bypass
- Wstępnie zdefiniowana konfiguracja ochrony
- Przechwytywanie pakietów zagrożeń w IPS (tylko z rozszerzeniem pojemności dysków)

Antivirus

- Ręczne, automatyczne push lub pull aktualizacji sygnatur
- Ręczne dodawanie lub usuwanie sygnatur MD5 do bazy danych AV
- Wysyłanie sygnatur MD5 do systemu sandbox w chmurze i ręczne dodawanie lub usuwanie w lokalnej bazie danych
- Antywirus oparty na przepływie (flow-based), obejmuje protokoły HTTP, SMTP, POP3, IMAP, FTP/SFTP, SMB
- Skanowanie skompresowanych plików pod kątem wirusów

Obrona przed atakami

- Ochrona protokołu przed atakiem bazująca na badaniu anormalnego zachowania
- Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood, fragmentacją TCP, fragmentacją ICMP itp.
- Obrona ataków na ARP
- Lista dozwolonych docelowych IP

Filtrowanie adresów URL

- Kontrola filtrowania web oparta na przepływie (flow-based)
- Ręczne definiowanie filtrowania web na podstawie adresu URL, zawartości strony web i nagłówka MIME
- Dynamiczne filtrowanie stron internetowych z chmurową bazą danych kategoryzacji w czasie rzeczywistym: ponad 140 milionów adresów URL w 64 kategoriach (z których 8 związanych jest z bezpieczeństwem)
- Dodatkowe funkcje filtrowania stron internetowych:
  - Filtrowanie apletu Java, ActiveX lub cookie
  - Blokowanie HTTP Post
  - Logowanie słów wyszukiwania
  - Wyłączanie skanowania zaszyfrowanych połączeń w stosunku do kategoriach w celu zachowania prywatności
- Nadpisywanie profilu filtrowania Web: umożliwia administratorowi tymczasowe przypisywanie różnych profili do użytkownika/grupy/adresu IP
- Nadpisywanie polityki filtracji o kategorie lokalną filtrowania web i ocenę kategorii
- Wsparcie dozwolonych i zablokowanych list URL

Antyspam

- Klasyfikacja i zapobieganie Spamowi w czasie rzeczywistym
- Potwierdzony Spam, Podejrzenie spamu, Masowy Spam, Poprawny Masowy Spam
- Ochrona Niezależnie od języka, formatu lub treści wiadomości
- Obsługa protokołów e-mail SMTP i POP3
- Wykrywanie ruchu przychodzącego i wychodzącego
- Whitelisty zezwalające na e-maile z zaufanych domen

Sandbox w chmurze

- Przekazywanie złośliwych plików do chmurowego sandbox w celu analizy
- Wsparcie protokołów takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB
- Obsługa typów plików jak PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów
- Kontrola kierunku transferu plików i rozmiaru pliku
- Dostarczanie pełnego raportu analizy zachowania dla złośliwych plików
- Globalna wymiana informacji o zagrożeniach, blokowanie zagrożeń w czasie rzeczywistym
- Obsługa trybu wykrywania bez przesyłania plików
- Konfiguracja dozwolonych i blokowanych list URL

Ochrona przez Botnet C&C

- Wyszukiwanie intranetowych hostów botnetu przez monitorowanie połączenia C&C i dalsze blokowanie zaawansowanych zagrożeń, takich jak botnet i ransomware
- Regularne aktualizowanie adresów serwerów botnetu
- Ochrona przez domenami i IP C&C
- Obsługa wykrywania ruchu TCP, HTTP i DNS
- Listy zezwalanych i blokowanych na podstawie adresu IP lub nazwy domeny
- Wykrywanie DNS sinkhole i DNS tunneling
- Obsługa wykrywania DGA

Reputacja IP

- Identyfikowanie i filtrowanie ruchu z ryzykownych adresów IP, takich jak hosty botnetów, spamerzy, węzły Tora, złośliwe hosty i ataki brute force
- Logowanie, drop pakietów lub blokowanie dla różnych typów ryzykownego ruchu IP
- Okresowe uaktualnianie bazy danych o sygnatury reputacji IP

Deszyfracja SSL/TLS

- Identyfikacja aplikacji dla ruchu szyfrowanego SSL/TLS
- Włączenie IPS dla ruchu szyfrowanego SSL/TLS
- Włączenie AV dla ruchu szyfrowanego SSL/TLS
- Filtrowanie adresów URL dla ruchu szyfrowanego SSL/TLS
- Whitelist dla zaszyfrowanego ruchu SSL/TLS
- Tryb proxy offlload SSL/TLS
- Obsługa identyfikacji aplikacji, DLP, IPS sandbox, AV dla proxy deszyfrowanego ruchu SMTPS/ POP3S/IMAPS

Identyfikacja i kontrola endpointów

- Obsługa identyfikacji adresu IP endpointów, ilości endpointów, czasu on-line, czasu off-line i zakresu czasu podłączenia on-line
- Obsługa 10 systemów operacyjnych, w tym Windows, iOS, Android, itp.
- Zapytania na podstawie adresu IP, liczby punktu końcowego, polityki kontroli i statusu itp.
- Obsługa identyfikacji ilości dostępnych endpointów w warstwie L3, logowanie o przekroczonych adresach IP
- Wyświetlanie strony przekierowania po niestandardowym zachowaniu
- Wsparcie dla operacji blokowania na przekroczonym IP
- Identyfikacja użytkownika i kontrola ruchu dla usług pulpitu zdalnego systemu Windows Server

Bezpieczeństwo danych

- Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy
- Identyfikacja protokołu plików zawierających HTTP, FTP, SMTP, POP3 i SMB
- Sygnatury plików i sufiksu dla ponad 100 typów plików
- Filtrowanie zawartości dla HTTP-GET, HTTP-POST, FTP i SMTP
- Identyfikacja i audyt zachowania sieci dla IM
- Filtrowanie plików przesyłanych przez protokół

Funkcje (Ciąg dalszy)

HTTPS przy użyciu SSL proxy oraz SMB

Kontrola aplikacji

- Ponad 4000 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka
- Każda aplikacja zawiera opis, czynniki ryzyka, zależności, typowe używane porty i adresy URL do dodatkowych odwołań
- Akcje: blokowanie, resetowanie sesji, monitorwanie, modelowanie ruchu
- Identyfikowanie i kontrolowanie aplikacji w chmurze
- Zapewnianie wielowymiarowego monitorowania i statystyk dla aplikacji w chmurze, w tym kategorii ryzyka i cech

Jakość usług (QoS)

- Maksymalna/gwarantowana przepustowość tuneli lub IP/użytkownik
- Alokacja tuneli na podstawie domeny bezpieczeństwa, interfejsu, adresu, użytkowników/ grupy użytkowników, serwera/ grupy serwerów, aplikacji/grupy aplikacji, TOS, sieci VLAN
- Przepustowość przydzielona na podstawie czasu, priorytetu lub równego udostępniania przepustowości
- Wsparcie Type of Service (TOS) i Differentiated Services (DiffServ)
- Priorytetowa alokacja pozostałej przepustowości
- Maksymalna liczba jednoczesnych połączeń na adres IP
- Alokacja przepustowości na podstawie kategorii URL
- Limit przepustowości w celu opóźnienia dostępu dla użytkownika lub adresu IP
- Automatyczne oczyszczanie po wygaśnięciu i ręczne oczyszczanie dla używanego ruchu przez użytkownika

Równoważenie obciążenia serwera

- Weighted hashing, weighted least-connection i weighted round-robin
- Przywiązanie sesji i monitorowanie stanu sesji
- Kontrola stanu zdrowia serwera (health check), monitorowanie sesji i ochrona sesji

Równoważenie obciążenia łącza

- Równoważenie obciążenia łącza dwukierunkowego
- Równoważenie obciążenia łącza wychodzącego: policy based routing, w tym ECMP, czas, ważony i osadzony routing usługodawcy. Aktywne i pasywne wykrywanie jakości łącza w czasie rzeczywistym i najlepszy wybór trasy
- Równoważenie obciążenia łącza przychodzącego obsługuje funkcję SmartDNS i wykrywanie dynamiczne
- Automatyczne przełączanie łączy w oparciu o przepustowość, opóźnienie, jitter, połączenia, aplikację itp.
- Inspekcja link health połączona z ARP, PING i DNS

VPN

- IPsec VPN
  - Tryb FAZY 1 IPSEC: aggressive i main ID protection mode
  - Opcje Peer acceptance: dowolny ID, określony ID, ID w grupie użytkowników dialup
  - Obsługuje IKEv1 i IKEv2 (RFC 4306)
  - Metody uwierzytelniania: certyfikat i klucz pre-shared
  - Obsługa konfiguracji trybu IKE (jako serwer lub klient)
  - Usługa DHCP przez protokół IPSEC
  - Konfigurowalne wygaśnięcie klucza szyfrowania IKE, NAT traversal keep alive traversal frequency
  - Propozycje szyfrowania dla Fazy 1/Fazy 2: DES, 3DES, AES128, AES192, AES256
  - Propozycje uwierzytelniania dla Fazy 1/Fazy 2: MD5, SHA1, SHA256, SHA384, SHA512
  - Obsługa dla IKE1 grup DH 1,2,5,19,20,21,24
  - Obsługa dla IKE2 grup DH 1,2,5,14,15,16,19,20,21,24
  - XAuth jako tryb serwera i dla użytkowników dialup
  - Wykrywanie nieaktywnego peer
  - Wykrywanie powtórek
  - Autokey keep-alive dla SA Fazy 2
- Obsługa IPSEC VPN realm: dozwalna wiele niestandardowych loginów SSL VPN skojarzonych z grupami użytkowników (ścieżki URL, design)
- Opcje konfiguracji VPN IPSEC: route-based lub policy based
- Tryby wdrażania VPN IPSEC: gateway-to-gateway, full mesh, hub-and-spoke, redundant tunnel, VPN termination in transparent mode
- Jednorazowe logowanie zapobiega równoczesnym logowaniu przy użyciu tej samej nazwy użytkownika
- Ograniczanie równoczesnych użytkowników do portalu SSL
- Moduł przekierowania portów VPN SSL szyfruje dane klienta i wysyła dane do serwera aplikacyjnego
- Obsługa klientów z systemem iOS, Android i Windows XP/Vista, w tym 64-bitowy system operacyjny Windows
- Wspiera sprawdzanie integralności hosta i sprawdzanie systemu operacyjnego przed połączeniami tunelowymi SSL
- Sprawdzanie adresu MAC hosta per portal
- Opcja czyszczenia cache przed zakończeniem sesji VPN SSL
- Tryb klienta i serwera L2TP, protokół L2TP over IPSEC i GRE over IPSEC
- Wyświetlanie i zarządzanie połączeniami IPSEC i SSL VPN
- PnPVPN
- VTEP dla VxLAN statyczny tunel unicastowy

IPv6

- Zarządzanie przez IPv6, logowanie IPv6 i HA
- Tunelowanie IPv6, DNS64/NAT64 , IPv6 ISATAP, IPv6 GRE, IPv6 over IPv4 GRE
- Routing IPv6, w tym routing statyczny, policy routing, ISIS, RIPng, OSPFv3 i BGP4+
- IPS, Identyfikacja aplikacji, Antywirus, kontrola dostępu, ochrona przed atakiem ND, iQoS
- Obsługa jumbo frames IPv6
- Obsługa Radius IPv6
- Obsługa protokołu IPv6 w następujących ALG: TFTP, FTP, RSH, HTTP, SIP
- Obsługa IPv6 w rozproszonym iQoS
- Wykrywanie śledzenia adresów

VSYS (dostępne tylko w modelach do montażu w szafie rack)

- Alokacja zasobów systemowych dla każdego VSYS
- Wirtualizacja CPU
- Non-root VSYS obsługuje firewall, IPSec VPN, SSL VPN, IPS, filtrowanie URL, reputację IP, AV, QoS
- Monitorowanie i statystyki VSYS, monitorowanie aplikacji, reputacja IP, AV, QoS

Wysoka dostępność (HA)

- Redundantne interfejsy z heartbeat
- Active/Passive i peer mode
- Indywidualne synchronizacje sesji
- Wydzielony interfejs HA
- Failover:
  - Monitorowanie portów oraz lokalnych i zdalnych linków
  - Stanowy failover
  - Przełączanie awaryjne poniżej sekundy
  - Powiadomienie o niepowodzeniu
- Opcje wdrażania:
  - HA z agregacją łączy
  - Full mesh HA
  - Geograficznie rozproszone HA
- Podwójne porty łącza danych HA

Twin-mode HA (dostępny tylko w modelu A3000 i wyższych modelach)

- Tryb wysokiej dostępności dla wielu urządzeń
- Wiele trybów wdrażania HA
- Konfiguracja i synchronizacja sesji pomiędzy wieloma urządzeniami

Identyfikacja użytkownika i urządzenia

- Lokalna baza danych użytkowników
- Zdalne uwierzytelnianie użytkowników: TACACS+, LDAP, Radius, Active Directory
- Single-sign-on (SSO): Windows AD
- Uwierzytelnianie dwuskładnikowe: wsparcie innych firm, zintegrowany serwer tokenów z fizyką i SMS
- Polityki oparte na użytkownikach i urządzeniach
- Synchronizacja grup użytkowników na podstawie AD i LDAP
- Obsługa 802.1X, SSO Proxy
- WebAuth: kastomizacja strony, ochrona przed force crack, obsługa IPv6
- Uwierzytelnianie oparte na interfejsie
- Bezagentowy ADSSO (AD Polling)
- Możliwosc synchronizacji uwierzytelniania opartej na SSO-monitor
- Wsparcie uwierzytelniania użytkowników opartego na adresach MAC i IP
- Serwer Radius wydający politykę bezpieczeństwa użytkownika za pośrednictwem wiadomości CoA

Administracja

- Dostęp do zarządzania: HTTP/HTTPS, SSH, telnet, konsola
- Zarządzanie centralne: Hillstone Security Manager (HSM), API web service
- Integracja systemu: SNMP, syslog, partnerstwa technologiczne
- Szybkie wdrożenie: automatyczna instalacja przez USB, lokalne i zdalne wykonywanie skryptów
- Dynamiczny dashboard w czasie rzeczywistym i monitorujące widżety z możliwością analizy w głąb (drill-down)

Funkcje (Ciąg dalszy)

- Język pomocy technicznej : angielski

Logowanie i raportowanie

- Możliwości logowania: Lokalny magazyn danych; do 6 miesięcy przechowywania logów z rozszerzeniem dysku (dysk twardy SSD), serwerem syslog, Hillstone HSM lub HSA
- Szyfrowanie logowania i integralności logów z zaplanowanym przekazywaniem batch log z HSA
- Niezawodne logowanie przy użyciu opcji TCP (RFC 3195)
- Szczegółowe logi z ruchu: przekazane, naruszone sesje, ruch lokalny, nieprawidłowe pakiety, adres URL itp.
- Kompleksowe zdarzenia logów: audyty aktywności systemowej i administracyjnej, routing i sieć, VPN, uwierzytelnianie użytkowników, zdarzenia związane z WiFi
- Opcjonalne rozwiazywanie nazw IP i usług
- Opcja krótkiego formatu logów dla ruchu
- Trzy wstępnie zdefiniowane raporty: Security, Flow i Network
- Raporty zdefiniowane przez użytkownika
- Raporty mogą być eksportowane w formacie PDF, Word i HTML za pośrednictwem poczty e-mail i FTP

Statystyka i monitorowanie

- Statystyki aplikacji, adresów URL i monitorowanych zagrożeń
- Statystyka i analizy ruchu w czasie rzeczywistym
- Informacje systemowe, takie jak jednoczesne sesje, CPU, pamięć i temperatura
- Statystyka ruchu i monitorowanie przez iQOS, monitorowanie stanu linków
- Zbieranie i przekierowywanie informacji o ruchu za pośrednictwem Netflow (wersja 9.0)

CloudView

- Monitorowanie zabezpieczeń z poziomu chmury
- 24/7 dostęp z web lub aplikacji mobilnej
- Monitorowanie stanu urządzenia, ruchu i zagrożeń
- Przechowywanie i retencja logów w chmurze

Specyfikacje

	SG-6000-A1000	SG-6000-A1100	SG-6000-A2000	SG-6000-A2600
				
Firewall Throughput [1]	4 Gbps	5 Gbps	5 Gbps	5 Gbps
NGFW Throughput [2]	1.2 Gbps	1.2 Gbps	1.2 Gbps	1.8 Gbps
Threat Protection Throughput [3]	800 Mbps	800 Mbps	800 Mbps	1.6 Gbps
Maximum Concurrent Sessions [4]	300,000	300,000	1 Million	1.2 Million
New Sessions/s [5]	48,000	48,000	48,000	120,000
IPS Throughput [6]	3.2 Gbps	3.2 Gbps	3.2 Gbps	4.5 Gbps
AV Throughput [7]	1.8 Gbps	2.0 Gbps	2.0 Gbps	3.7 Gbps
Virtual Systems (Default/Max)	N/A	N/A	1/5	1/5
Management Ports	1 × Console Port, 2 × USB3.0 Port	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45)
Fixed I/O Ports	4 × GE	8 × GE (including 1 bypass pair)	8 × GE (including 1 bypass pair)	8 × GE (including 1 bypass pair)
Available Slots for Expansion Modules	N/A	N/A	N/A	N/A
Expansion Module Option	N/A	N/A	N/A	N/A
Twin-mode HA	N/A	N/A	N/A	N/A
Local Storage	8 GB	8 GB	8 GB	8 GB
Expansion Storage Options	256 GB SSD	256 GB SSD	480 GB / 960 GB / 1.92 TB SSD	480 GB / 960 GB / 1.92 TB SSD
Power Specification	30W, Single AC	50W, Single AC	50W, Single AC (default), Dual AC (optional)	50W, Single AC (default), Dual AC (optional)
Power Supply	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V
Form Factor	Desktop	Desktop	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	270 × 160 × 44	270 × 160 × 44	436 × 320 × 44	436 × 320 × 44
Dimensions (W × D × H, inches)	10.6 × 6.3 × 1.7	10.6 × 6.3 × 1.7	17.2 × 12.6 × 1.7	17.2 × 12.6 × 1.7
Weight	3.1 lb (1.4 kg)	3.1 lb (1.4 kg)	8.6 lb (3.9 kg)	8.6 lb (3.9 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

Specyfikacje (Ciąg dalszy)

	SG-6000-A3000	SG-6000-A3600	SG-6000-A3700	SG-6000-A3800
				
Firewall Throughput [1]	20 Gbps	20 Gbps	20 / 40 Gbps	20 / 40 Gbps
NGFW Throughput [2]	1.8 Gbps	1.8 Gbps	1.8 Gbps	3.7 Gbps
Threat Protection Throughput [3]	1.6 Gbps	1.6 Gbps	1.6 Gbps	2.8 Gbps
Maximum Concurrent Sessions [4]	2 Million	3 Million	6 Million	8 Million
New Sessions/s [5]	140,000	140,000	140,000	310,000
IPS Throughput [6]	8.3 Gbps	8.5 Gbps	8.6 Gbps	17.5 Gbps
AV Throughput [7]	4.8 Gbps	5.0 Gbps	5.2 Gbps	9.4 Gbps
Virtual Systems (Default/Max)	1/5	1/50	1/100	1/100
Management Ports	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)
Fixed I/O Ports	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)
Available Slots for Expansion Modules	N/A	N/A	1	1
Expansion Module Option	N/A	N/A	IOC-A-4SFP+, IOC-A-2MM-BE, IOC-A-2SM-BE	IOC-A-4SFP+, IOC-A-2MM-BE, IOC-A-2SM-BE
Twin-mode HA	Yes	Yes	Yes	Yes
Local Storage	8 GB	8 GB	8 GB	8 GB
Expansion Storage Options	480 GB / 960 GB / 1.92 TB SSD	480 GB / 960 GB / 1.92 TB SSD	480 GB / 960 GB / 1.92 TB SSD	480 GB / 960 GB / 1.92 TB SSD
Power Specification	100W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	100W, Dual AC (default), Dual DC (optional)
Power Supply	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V
Form Factor	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	436 × 437 × 44	436 × 437 × 44	436 × 437 × 44	436 × 437 × 44
Dimensions (W × D × H, inches)	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7
Weight	13.2 lb (6 kg)	13.2 lb (6 kg)	13.4 lb (6.1 kg)	15 lb (6.8 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

Opcjonalne moduły

	IOC-A-4SFP+	IOC-A-2MM-BE	IOC-A-2SM-BE
			
Names	4SFP+ Expansion Module	4SFP Multi-mode Bypass Expansion Module	4SFP Single-mode Bypass Expansion Module
I/O Ports	4 × SFP+, SFP+ module not included	4 × SFP, MM bypass (2 pairs of bypass ports)	4 × SFP, SM bypass (2 pairs of bypass ports)
Dimension	1U	1U	1U
Weight	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)

Notatki:

(1) Dane dotyczące przepustowości firewall uzyskiwane są z ruchu UDP o rozmiarze pakietu 1518 bajtów. Przepustowość Firewall dla modeli A3700 i A3800 można zwiększyć z 20 Gb/s do 40 Gb/s za pomocą dodatkowego modułu rozszerzającego IOC-A-4SFP+;

(2) Przepustowość danych NGFW uzyskiwana jest w stosunku do ruchu 64 Kbajtów HTTP z włączoną kontrolą aplikacji i włączonym IPS;

(3) Przepustowość danych Threat protection uzyskiwana jest w stosunku do ruchu 64 Kbajtów HTTP z włączoną kontrolą aplikacji, IPS, AV i filtrem URL;

(4) Maksymalna liczba równoczesnych sesji pozyskiwania jest w ramach ruchu HTTP;

(5) Nowe sesje/sekundę uzyskiwane są w ramach ruchu TCP;

(6) Przepustowość danych IPS uzyskiwane jest w trybie dwukierunkowego wykrywania ruchu HTTP z włączonymi wszystkimi regułami IPS;

(7) Przepustowość danych AV uzyskiwane jest w ramach ruchu HTTP z załącznikiem pliku.

O ile nie określono inaczej, wszystkie wydajności, pojemności i funkcjonalności oparte są na StoneOS5.5R8. Wyniki mogą się różnić w zależności od wersji wdrożenia StoneOS®.

Version: EX-08.01-NGFW-A-Series-5.5R8-0221-PL-03