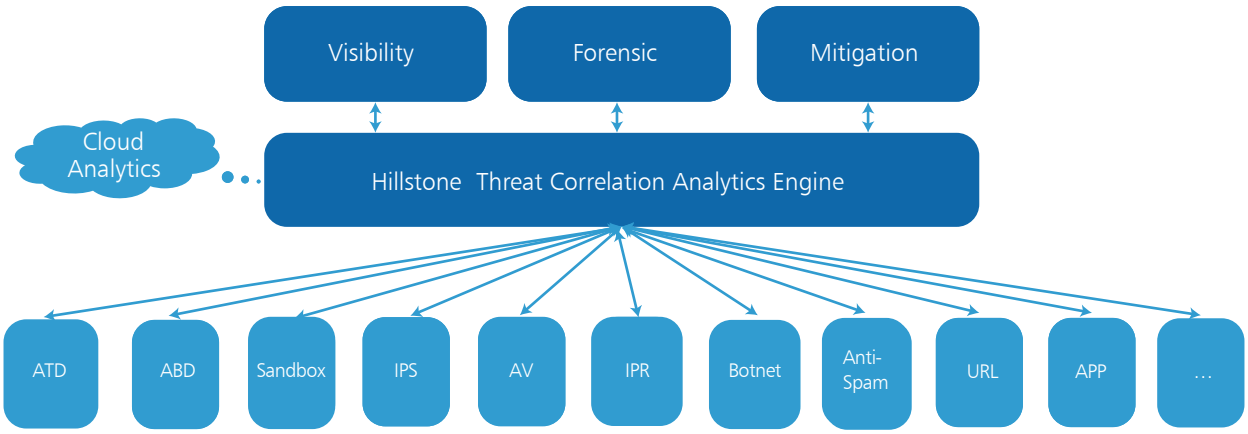
Hillstone Seria T

Inteligentne Firewall Nowej Generacji

Inteligentny Firewall Nowej Generacji (iNGFW) firmy Hillstone wykorzystuje trzy kluczowe technologie do wykrywania zaawansowanych ataków i ciągłej ochrony przed zagrożeniami w sieciach. Pierwsza, wykorzystuje algorytmy klastrów statystycznych w celu wykrywania nieznanego złośliwego oprogramowania poprzez opatentowany silnik Advanced Threat Detection (ATD). Druga, używa analizy behawiorystycznej do wykrywania nietypowego zachowania w sieciach, która oparta jest na Hillstone Abnormal Behavior Detection (ABD). Wreszcie trzecia, wykorzystuje silnik analizy korelacji zagrożeń Hillstone do korelowania wykrytych zagrożeń przez różne silniki - w tym ATD, ABD, Sandbox oraz inne tradycyjne technologie wykrywania zagrożeń oparte na sygnaturach dołączając do tego informacje kontekstowe w celu identyfikacji zaawansowanych zagrożeń.

Dzięki funkcjonalności głębokiego wykrywania i analizy zagrożeń, Hillstone iNGFW zapewnia klientom kompleksową widoczność oceny ryzyka sieciowego, a także szczegóły zagrożenia dla każdego hosta. Hillstone INGFW dostarcza administratorom informacje kryminalistyczne z różnych narzędzi i ścieżek, aby przejść do analizy w głąb i znaleźć źródło ataku. Ponadto, Hillstone iNGFW dostarcza administratorom potężne funkcje mitygacji, które dają czas administratorom do zbadania danych kryminalistycznych, podjęcia świadomej decyzji o autentyczności ataku i zminimalizowania szkód biznesowych.



Najważniejsze informacje o produktach

Wykrywanie nieznanego złośliwego oprogramowania

Hillstone zbudował opatentowany silnik, który przeanalizował blisko milion „znanych" próbek złośliwego oprogramowania. Każda próbka została sklasyfikowana i scharakteryzowana na podstawie wielu wymiarów opisujących jego działanie, zasoby i atrybuty. Każda nowa próbka pojawiająca się w środowisku produkcyjnym jest również analizowana, scharakteryzowana i klasyfikowana. Następnie porównywana jest do bazy znanych próbek złośliwego oprogramowania, które zostały wcześniej przeanalizowane. Im bliżej nieznana próbka odpowiada znanej próbce — tym daje do większą pewność, że jest to wariant znanego złośliwego oprogramowania. Proces ten nazywany jest „klastrowaniem statystycznym" i zapewnia dokładną metodę identyfikacji nowego złośliwego oprogramowania.

Wykrywanie nietypowego zachowania

Silnik Hillstone Abnormal Behavior stale uczy się sieci, aby dowiedzieć się, jak wygląda normalny ruch sieciowy dla danego dnia i czasu. Alertuje na podstawie zbadanego ruchu, gdy aktywność sieciowa przekracza obliczone progi. Używa do tego celu ponad 50 tablic wymiarowych, które służą do kalkulowania normalnego ruchu sieciowego w warstwach L4-L7. Proces ten określany jest jako "modelowanie zachowania". Dodatkowo został on przeszkolony prawdziwymi narzędziami hakerskimi w celu zapewnienia, że szkodliwe działania będą prawidłowo rozpoznawane. Techniki te ograniczają liczbę false positive i zapewniają użytkownikowi wiele możliwości zatrzymania ataku.

Bogata Analiza Kryminalistyczna (Forensic)

Hillstone oferuje nowy sposób wizualizacji i analizowania ataków. Każde działanie podjęte przez potencjalnie złośliwy kod jest automatycznie połączone z krokami w ramach "Kill Chain". Jest on uzupełniony bogatymi informacjami kryminalistycznymi, które umożliwiają analitykowi bezpieczeństwa określenie pochodzenia ataku, dotkliwości ataku i zastosowanej metodologii. Hillstone dostarcza również przechwytywanie pakietów. Połączenie ich z syslog i logami z ruchu, dostarcza administratorowi bogate informacje dodatkowe. Ponadto dane użytkowników takie jak odwiedzane strony web, używane aplikacje i poziom ryzyka aplikacji, wyostrza informacje o exploitach. Co najważniejsze, Hillstone identyfikuje i wyróżnia dokładne polityki firewall, które pozwoliły atakującemu przedostać się przez zabezpieczenia.

Zapobiegawcza mitygacja

Aby zapobiec atakowi, oprócz możliwości zmiany polityk, Hillstone posiada kilka wbudowanych funkcji automatycznej mitygacji. Funkcje te składają się ze wstępnie zdefiniowanych szablonów, które automatycznie spowalniają lub blokują atak w przypadku wykrycia podejrzanego zachowania. Administrator może zmodyfikować szablony, aby ograniczyć przepustowość lub liczbę sesji dostępnych dla osoby atakującej. Na podstawie rodzaju ataku i poziomu nasilenia możliwe jest również dostosowanie ograniczenia, które nakładane są na zasoby sieciowe. W przypadkach, gdy atak jest krytycznego poziomu i dotyka danych poufnych, mitygacja może obejmować całkowite zablokowanie wszystkich zasobów sieciowych. A jeśli szablon nie istnieje lub nie jest aktywny, administrator może szybko skonfigurować tymczasowe ograniczenie dla takiego zdarzenia.

Funkcje

Analiza korelacji zagrożeń
- Korelacja między nieznanymi zagrożeniami, nieprawidłowym zachowaniem i zachowaniem aplikacji w celu wykrycia potencjalnego zagrożenia lub ataków
- Reguły korelacji wielowymiarowej, automatyczna codzienna aktualizacja z chmury

Zaawansowane wykrywanie zagrożeń
- Zaawansowane wykrywanie złośliwego oprogramowania oparte na badaniu zachowania
- Wykrywanie ponad 2000 znanych i nieznanych rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów, itp.
- Aktualizowanie bazy danych modelu zachowania złośliwego oprogramowania w czasie rzeczywistym i online

Wykrywanie anormalnego zachowania
- Modelowanie zachowania oparte na baseline ruchu L3-L7 w celu ujawnienia anomalnych zachowań sieciowych, takich jak skanowanie HTTP, Spider, SPAM, słabe hasła SSH/FTP itp.
- Wykrywanie DDoS w tym Flood, Sockstress, zip od death, ataków typu reflect, zapytań DNS, SSL DDoS i aplikacyjnego DDoS
- Obsługa inspekcji szyfrowanego ruchu tunelowego do nieznanych aplikacji
- Wykrywanie ataku C&C przy użyciu algorytmu generowania domeny (DGA)
- Aktualizacja bazy danych modelu anormalnego zachowania w czasie rzeczywistym oraz online

Widoczność zagrożeń i łagodzenie ich skutków
- Ocena ryzyka, krytyczność zasobu i status ryzyka hosta, dotkliwość i pewność zagrożenia
- Mapowanie zagrożenia na zdarzenia kill chain dla każdego hosta
- Forensic zagrożenia w tym analiza zagrożenia, bazy wiedzy, historia i PCAP
- Wstępnie zdefiniowane i dostosowane reguły mitygacji
- Obsługa whitelist zagrożeń

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 – łączenie do SPAN portu
- Tryby interfejsu: sniffer, agregowane portów, loopback, VLANy (802.1Q i Trunking)
- L2/L3 routing i switching
- 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 centralną tablicę NAT
- VoIP: SIP/H.323/SCCP NAT traversal, RTP ping holing
- Widok globalnego zarządzania politykami
- Inspekcja nadmiarowości polityk bezpieczeństwa, polityki grupowe przywracanie konfiguracji polityk (rollback)
- Asystent Polityk dla ułatwienia szczegółowego wdrażania polityk
- Analiza polityk i czyszczenie nieprawidłowych polityk
- Kompleksowe polityki DNS
- Harmonogramy: jednorazowe i cykliczne

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 szczególnych 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, z ICMP sweep, TCP/UDP/ SCIP/ICMP flooding sesji (źródło/cel)
- Aktywny bypass z interfejsami bypass
- Wstępnie zdefiniowana konfiguracja ochrony

Antywirus
- Ręczne, automatyczne push lub pull aktualizacje sygnatur
- Wysyłanie MD5 sygnatury do systemu sandbox w chmurze i ręczne dodawanie lub usuwanie w lokalnej bazie danych
- Program antywirusowy 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, fragmentację TCP, fragmentację 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 jest związanych 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
- Konfiguracja list blokowania/dozwalania URL

Ochrona przed spamem
- Ochrona przed Spamem i klasyfikacja Spamu w czasie rzeczywistym
- Potwierdzony Spam, podejrzany Spam, objętościowy Spam, prawidłowy Spam zbiorczy
- Ochrona Niezależnie od języka, formatu lub zawartości wiadomości email
- Obsługa jednocześnie protokołów poczty e-mail SMTP i POP3
- Wykrywanie ruchu przychodzącego i wychodzącego
- White-list umożliwiające wysyłanie wiadomości e-mail z zaufanych domen

Sandbox w chmurze
- Przekazywanie złośliwych plików do sandbox chmury w celu analizy
- Wsparcie protokołów w tym 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

Ochrona przed Botnet C&C
- Wyszukiwanie intranetowych hostów bitnetu 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

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

Funkcje (Nieprzerwany)

- Filtrowanie adresów URL dla ruchu szyfrowanego SSL/TLS
- Whitelist dla zaszyfrowanego ruchu SSL/TLS
- Tryb proxy offlload SSL/TLS

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.
- Zapylanie na podstawie adresu IP, liczby punktu końcowego, polityki kontroli i statusu itp.
- Obsługa identyfikacji ilości dostępnych endpointów w warstwie 3, logowanie i o przekroczonych adresów 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
- Identyfikacja i audyt zachowania sieci dla IM
- Filtrowanie plików przesyłanych przez protokół HTTPS przy użyciu SSL proxy oraz SMB

Kontrola aplikacji

- Ponad 3000 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, monitorowanie, 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 Typu 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: dozwala 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

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 (WSO)

- 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

Wysoka dostępność (HA)

- Redundantne interfejsy z heartbeat
- Tryby Aktywny/Aktywny i Aktywny/Pasywny
- 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

Identyfikacja użytkownika i urządzenia

- Lokalna baza danych użytkowników
- Zdalne uwierzytelnianie użytkowników: TACACS+, LDAP, Radius, Active
- 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)

Funkcje (Nieprzerwany)

- Możliwość synchronizacji uwierzytelniania opartej na SSO-monitor
- Wsparcie uwierzytelniania użytkowników opartego na adresach MAC i IP

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 w możliwością analizy w głąb (drill-down)
- Język pomocy technicznej: angielski

Logowanie i raportowanie

- Możliwości logowania: pamięć lokalna i pamięć masowa (jeśli są dostępne), wiele serwerów syslog i wiele platform Hillstone Security Audit (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
- Opcja 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

Statystyki i monitorowanie

- Statystyki aplikacji, adresów URL i monitorowanych zagrożeń
- Statystyka ruchu w czasie rzeczywistym i analizy
- 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-T1860	SG-6000-T2860	SG-6000-T3860	SG-6000-T5060	SG-6000-T5860
					
Przepustowość FW [1]	8 Gb/s	10 Gb/s	20 Gb/s	25 Gb/s	40 Gb/s
Przepustowość IPS [2]	3 Gb/s	4 Gb/s	8 Gb/s	12 Gb/s	18 Gb/s
Przepustowość AV [3]	1.6 Gb/s	2 Gb/s	6 Gb/s	7 Gb/s	10 Gb/s
Przepustowość protokołu IPSec [4]	3 Gb/s	3.8 Gb/s	12 Gb/s	15 Gb/s	28 Gb/s
Przepustowość IMIX [5]	1.6 Gb/s	2.1 Gb/s	8.2 Gb/s	10.9 Gb/s	17.4 Gb/s
Przepustowość NGFW [6]	1 Gb/s	1.5 Gb/s	5 Gb/s	8 Gb/s	12 Gb/s
Przepustowość ochrony przed zagrożeniami [7]	600 Mb/s	900 Mb/s	2.5 Gb/s	4 Gb/s	6 Gb/s
Nowe sesje/sesje [8]	80,000	100,000	250,000	300,000	450,000
Maksymalna liczba równocze-snych sesji [9]	1.5 miliony	3 miliony	4 miliony	5 milionów	6 milionów
Ilość tuneli IPSec	6,000	10,000	20,000	20,000	20,000
Użytkownicy sieci VPN SSL (do-myślnie/maks.)	8 / 4,000	8 / 6,000	128 / 10,000	128 / 10,000	128 / 10,000
Wirtualne Systemy (domyślne/ maks.)	1 / 50	1 / 50	1 / 100	1 / 250	1 / 250
Stałe porty we/wy	6 × GE, 4 × SFP	6 × GE(1 pair bypass port), 4 × SFP, 2 × SFP+	2 × GE, 4 × SFP	2 × GE, 4 × SFP	2 × GE, 4 × SFP
Maksymalna liczba we/wy	26 × GE	26 × GE, 2 × 10GE	22 × GE, 4 × 10GE	38 × GE, 8 × 10GE	38 × GE, 16 × 10GE
Dostępne sloty dla Modułów Rozszerzeń	2 × ogólne gniazdo	2 × ogólne gniazdo	2 × ogólne gniazdo	4 × ogólne gniazdo	4 × ogólne gniazdo
Opcja modułu rozszerzeń	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M, IOC-2SFP+-Lite	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-8SFP+, IOC-4SFP+, IOC-2SFP+-Lite	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-8SFP+, IOC-4SFP+, IOC-2SFP+-Lite
Porty zarządzania	1 × Concole Port, 1 × HA, 1 × MGT, 1 × USB 2.0, 1 × AUX Port	1 × Concole Port, 1 × HA, 1 × MGT, 1 × USB 2.0, 1 × AUX Port	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT
Specyfikacja zasilania	150W, pojedynczy AC lub DC, podwójny nadmiar-owy AC	150W, pojedynczy AC lub DC, podwójny nadmiarowy AC	450W, podwójny nadmiarowy AC lub dual DC	450W, podwójny nadmiarowy AC lub dual DC	450W, podwójny nadmiarowy AC lub dual DC
Opcje przechowywania	480G SSD (opcjonalnie 960G SSD)	480G SSD (opcjonalnie 960G SSD)	Podwójna magazyn danych: 120G (opcjonalnie 480G lub 960G SSD) +480G SSD (opcjonalnie 960G SSD)	Podwójna magazyn danych: 120G (opcjonalnie 480G lub 960G SSD) +480G SSD (opcjonalnie 960G SSD)	Podwójna pamięć masowa: 120G (opcjonalnie 480G lub 960G SSD) +1T
Zasilanie	AC 100-240 V 50/60 Hz DC -40 ~ -60 V	AC 100-240 V 50/60 Hz DC -40 ~ -60 V	AC 100-240 V50/60 Hz DC -40 ~ -60 V	AC 100-240 V 50/60 Hz DC -40 ~ -60 V	AC 100-240 V 50/60 Hz DC -40 ~ -60V
Wymiar (S×D×W mm)	1 U 17,2 x 14,4 x 1,7 cala (436 x 366 x 44 mm)	1 U 17,2 x 14,4 x 1,7 cali (436 x 366 x 44 mm)	2 U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)	2 U 17,3 × 20,5 × 3,5 cala (440 × 520 × 88 mm)	2 U 17,3 × 20,5 × 3,5 cala (440 × 520 × 88 mm)
Waga	12,3 funta (5,6 kg)	12,3 funta (5,6 kg)	34,2 funta (15,5 kg)	34,8 funta (15,8 kg)	34,8 funta (15,8 kg)
Temperatura	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Wilgotność względna	10-95% (bez rosy)	10-95% (bez rosy)	10-95% (bez rosy)	10-95% (bez rosy)	10-95% (bez rosy)
Zgodność i certyfikaty	CE, CB, FCC, UL/cUL, ROHS, IEC/EN61000-4-5 Power Surge Protection, ISO 9001:2015, ISO 14001:2015, CVE Compatibility, IPv6 Ready, ICSA Firewalls				

Wersja: EX-08.01-iNGFW-5.5R8-0121-PL-01

Opcjonalne moduły

	IOC-8GE-M	IOC-8SFP-M	IOC-4GE-B-M	IOC-2SFP+-Lite	IOC-8SFP+	IOC-4SFP+
						
Nazwa	Moduł rozszerzający 8GE	Moduł rozszerzeń 8SFP	Moduł rozszerzający obejście 4GE	Moduł rozszerzeń 2SFP+	Moduł rozszerzeń 8SFP+	Moduł rozszerzeń 4SFP+
Porty we/wy	8 x GE	8 x Moduł SFP, SFP nie jest dołączony	4 x GE Bypass (2 parowe porty obejściowe)	2 x Moduł SFP+, SFP+ nie jest dołączony	8 X moduł SFP+, SFP+ nie jest dołączony	4 x moduł SFP+, SFP+ nie jest dołączony
Wymiar	1/2 U (zajmuje 1 ogólne gniazdo)	1/2 U (zajmuje 1 slot)	1/2 U (zajmuje 1 ogólne gniazdo)	1/2 U (zajmuje 1 slot)	1 U (zajmuje 2 gniazda ogólne)	1 U (zajmuje 2 gniazda ogólne)
Waga	1,8 lb (0,8 kg)	2,0 lb (0,9 kg)	1,8 lb (0,8 kg)	0,7 lb (0,3 kg)	1,5 lb (0,7 kg)	1,5 lb (0,7 kg)

Notatki:

(1) Przepustowość danych FW uzyskiwana jest w ramach pojedynczego stosu ruchu UDP o rozmiarze pakietu 1518 bajtów;
(2) Przepustowość danych IPS uzyskiwane jest w trybie dwukierunkowego wykrywania ruchu HTTP z włączonymi wszystkimi regułami IPS;
(3) Przepustowość danych AV uzyskiwane jest w ramach ruchu HTTP z załącznikiem pliku;
(4) Przepustowość danych IPSec uzyskiwana jest w konfiguracji Preshare Key AES256+SHA-1 i 1400-bajtowym rozmiarze pakietu;
(5) Przepustowość danych IMIX uzyskiwana jest w ramach ruchu mieszanego UDP (64 bajty: 512 bajtów: 1518 bajtów = 5:7:1);
(6) Przepustowość danych NGFW uzyskiwana jest w stosunku do ruchu 64 Kbajtów HTTP z włączoną kontrolą aplikacji i włączonym IPS;
(7) Przepustowość danych Threat protection uzyskiwana jest w stosunku do ruchu 64 Kbajtów HTTP z włączoną kontrolą aplikacji, IPS, AV i filtrem URL;
(8) Nowe sesje/sekundę uzyskiwane są w ramach ruchu HTTP;
(9) Maksymalna liczba równoczesnych sesji pozyskiwania jest w ramach ruchu HTTP.
O ile nie określono inaczej, wszystkie wydajności, pojemności i funkcjonalności oparte są na StoneOS5.5R8. Wyniki mogą się różnić w zależności od wersji wdrożenia Stones®.

Wersja: EX-08.01-iNGFW-5.5R8-0121-PL-01