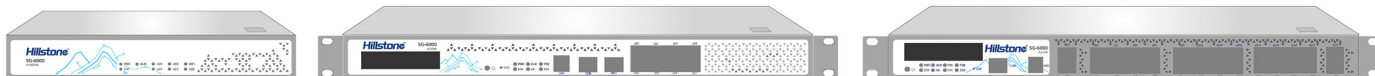


Hillstone A-Series

Next-Generation Firewall



O firewall de próxima geração Hillstone A-Series oferece alto desempenho de segurança, expansão conforme necessário, detecção e prevenção de ameaças avançadas completas e operação de política inteligente e automatizada. Esta série NGFW, pronta para o futuro, é baseada em uma arquitetura de hardware totalmente nova que oferece desempenho de camada de aplicativo líder do setor para atender às necessidades de segurança de rede do mundo real. Portas de alta densidade garantem excelente capacidade de acesso e grandes opções de armazenamento oferecem melhor visibilidade e análise. O Hillstone A-Series NGFW oferece defesas avançadas completas contra ameaças conhecidas e desconhecidas, juntamente com uma operação de política inteligente, automatizada e eficiente que facilita as operações de segurança.

Destaques do Produto

Detecção e proteção avançada de ameaças

O Hillstone A-Series NGFW inclui um conjunto completo de mecanismos para fornecer detecção e proteção em tempo real em todo o ciclo de vida de ataques de rede e malwares. Antes que uma violação possa ocorrer, proteções pró-ativas como o IPS bloqueiam a exploração de vulnerabilidades. Os serviços de reputação de IP bloqueiam solicitações de sites arriscados potencialmente envolvidos em malware e spamming. A filtragem de URL impede que os usuários acessem inadvertidamente sites associados a phishing, downloads de malware e outras explorações. O antivírus detecta e bloqueia malwares conhecidos no nível da rede com um banco de dados de assinatura avançado que é atualizado continuamente. O anti-spam fornece classificação e prevenção de spam em tempo real para o tráfego de entrada e saída. Durante uma violação, o antivírus também desempenha

um papel importante, continuando a detectar e bloquear malwares conhecidos. Uma sandbox em nuvem fornece detecção e prevenção sofisticadas de arquivos maliciosos por meio de análise estática e pré-processamento, seguido por análise comportamental que inclui detecção de manobras evasivas. A inteligência em nuvem identifica e bloqueia arquivos maliciosos, gera logs e relatórios e compartilha inteligência de ameaças com a nuvem.

Completando as proteções em todo o ciclo de vida da ameaça, a Série A continua a se defender, mesmo após a ocorrência de uma violação. O recurso avançado de prevenção de Botnet C&C da Hillstone impede a comunicação com o canal de controle e também detecta e bloqueia bots dentro da intranet.

Além disso, o mecanismo unificado de detecção e análise de ameaças do sistema é coordenado por todos os mecanis-

Destaques do Produto (Contínua)

mos de segurança integrados para aumentar drasticamente a eficiência, reduzindo a latência da rede.

Arquitetura de Hardware de Alto Desempenho

A série A, preparada para o futuro, apresenta um formato compacto e uma base de computação poderosa que garante alto desempenho com segurança absoluta. Os NGFWs da série A oferecem desempenho robusto para rendimento de firewall, sessões simultâneas e novas, e desempenho extremamente rápido para a camada de aplicativo, o que é crítico para atender às necessidades dos ambientes de segurança atuais. Ele também oferece uma ecologia de software amigável para integração de terceiros para oferecer suporte a recursos de segurança adicionais, se desejado. Todos os modelos de montagem em rack apresentam ventilação frontal e traseira para auxiliar na dissipação de calor, o que é uma preocupação em redes de quase todos os tamanhos.

Excelente capacidade de acesso e expansão de armazenamento

O Hillstone A-Series oferece alta densidade de portas de E/S, permitindo que o NGFW atue como um switch ou roteador conforme necessário, reduzindo os custos de implantação e gerenciamento. Além disso, slots de expansão estão disponíveis para vários modelos da Série A para aumentar ainda mais o desempenho. Os pares de bypass na maioria dos modelos da série A ajudam a garantir a continuidade dos negócios.

Todos os modelos, incluindo as versões de desktop, incluem um grande armazenamento integrado de 8 GB e têm opções de expansão para armazenamento em disco rígido muito grande de até 2 TB. Com mais armazenamento, o sistema pode salvar mais logs e dados por mais tempo, permitindo uma análise mais profunda. Além disso, o armazenamento expandido permite que o sistema forneça relatórios mais ricos com muito mais informações, incluindo resultados

visualizados e recomendações acionáveis.

Além disso, com uma análise de ameaças mais profunda, o WebUI pode exibir informações de detecção de ameaças muito mais ricas, o que, por sua vez, dá aos administradores melhor visibilidade. A maior visibilidade permite que os administradores localizem rapidamente anomalias e outros eventos de rede ou tráfego suspeitos, analisem-nos e respondam.

Operação de Política Inteligente

A série A inclui gerenciamento e operação inteligentes em todo o ciclo de vida da política, desde a implantação até o gerenciamento, otimização e operação. O sistema oferece implantação de política de usuário automatizada usando autorização dinâmica RADIUS. O gerenciamento de políticas é muito mais eficiente por meio de agrupamentos de políticas com base nos requisitos de negócios. Além disso, as políticas podem ser agregadas para permitir que um conjunto de políticas atue como uma única política. Um assistente de política inovador analisa os padrões de tráfego e recomenda políticas refinadas para um gerenciamento de políticas mais rápido, fácil e preciso. A operação da política se torna mais eficiente e precisa por meio de verificações de redundância de política, que identificam políticas redundantes para desativação ou exclusão, e análise de contagem de acertos de política, que ajuda a refinar e ajustar as políticas.

Recursos

Serviços de Rede

- Roteamento dinâmico (OSPF, BGP, RIPv2)
- Roteamento estático e por política
- Roteamento controlado pela aplicação
- DHCP, NTP, Servidor DNS e proxy DNS incorporados
- Modo tap - conecta-se à porta SPAN
- Modos de interface: sniffer, porta agregada, loopback, VLANS (802.1Q e Trunking)
- Comutação e roteamento L2/L3
- Multicast (PIM-SSM)
- Implementação em linha transparente wire virtual (Camada 1)

Firewall

- Modos de operação: NAT/rota, transparente (ponte) e modo misto
- Objetos de políticas: predefinidos, personalizados, política agregada, agrupamento de objetos
- Política de segurança com base na aplicação, função e geolocalização
- Suporte a Gateways de Nível de Aplicação e sessão: MSRCP, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, dcerpc, dns-tcp, dns-udp, H.245 0, H.245 1, H.323
- Suporte a NAT e ALG: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN
- Configuração NAT: por política e tabela central de NAT
- VoIP: SIP/H.323/SCCP NAT traversal, RTP pin holing
- Visualização de gerenciamento global de política
- Inspeção de redundância de política de segurança, grupo de política, política agregada de reversão de configuração de política
- Assistente de Políticas para fácil implantação detalhada de políticas
- Análise de políticas e limpeza de políticas inválidas
- Política abrangente de DNS
- Programações: única e recorrente
- Apoio à importação e exportação de políticas

Prevenção de Intrusão

- Detecção de anomalia de protocolo, detecção baseada em taxa, assinaturas personalizadas, atualizações de assinatura push ou pull manual e automática, enciclopédia de ameaça integrada
- Ações de IPS: padrão, monitorar, bloquear, redefinir (IP do atacante ou IP da vítima, interface de entrada) com tempo de expiração
- Opção de registro de pacote
- Seleção Baseada em Filtro: gravidade, destino, SO, aplicação ou protocolo
- Isenção de IP de assinaturas IPS específicas
- Modo sniffer IDS
- Proteção contra DoS baseada em taxa de IPv4 e IPv6 com definições de limite contra TCP Syn flood, varredura de porta TCP/UDP/SCTP, varredura ICMP, TCP/UDP/SCIP/ICMP session flooding (origem/destino)
- Bypass ativo com interfaces de bypass
- Configuração de prevenção predefinida
- Captura de pacotes de ameaças IPS (apenas com armazenamento de expansão)

Antivírus

- Atualizações de assinatura push ou pull manual e automática
- Adicionar ou excluir manualmente a assinatura

MD5 do banco de dados AV

- Suporta a assinatura MD5, upload para nuvem sandbox e adição ou eliminação no banco de dados local
- Antivírus baseado em fluxo: os protocolos incluem HTTP, SMTP, POP3, IMAP, FTP / SFTP e SMB
- Varredura de vírus em arquivo compactado

Contra-ataque

- Contra-ataque de protocolo anormal
- Anti-DoS / DDoS, incluindo inundações de SYN, inundações de UDP, inundações de resposta DNS, defesa de inundações de consulta DNS, fragmento TCP, fragmento ICMP, etc.
- Contra-ataque de ARP
- Lista de permissões para endereço IP de destino

Filtro de URL

- Inspeção de filtro de Web baseada em fluxo
- Filtro de Web definido manualmente baseado em URL, conteúdo da Web e cabeçalho MIME
- Filtro dinâmico de Web com banco de dados de categorização em tempo real baseada na nuvem: mais de 140 milhões de URLs com 64 categorias (8 das quais relacionadas a segurança)
- Recursos de filtro de Web adicionais:
 - Filtrar Java Applet, ActiveX ou cookie
 - Bloquear post HTTP
 - Registrar palavras-chave de busca
 - Isentar conexões de varredura criptografadas em certas categorias para privacidade
- Substituição de perfil de filtro de Web: permite que o administrador atribua temporariamente diferentes perfis a usuário/grupo/IP
- Substituição de categorias locais e de classificação de categoria de filtro de Web
- Apoio, suporte Lista de permissão de URL e lista de bloqueio

Anti-Spam

- Classificação e prevenção de spam em tempo real
- Spam confirmado, spam suspeito, spam em massa, volume válida
- Proteção, independentemente do idioma, formato ou conteúdo da mensagem
- Suporta os protocolos de e-mail SMTP e POP3
- Detecção de entrada e saída
- Listas brancas para permitir e-mails de domínios confiáveis

Sandbox de Nuvem

- Carregamento de arquivos maliciosos em sandbox de nuvem para análise
- Suporte para protocolos, incluindo HTTP/HTTPS, POP3, IMAP, SMTP, FTP e SMB
- Suporta tipos de arquivo, incluindo PE, ZIP, RAR, Office, PDF, APK, JAR, SWF e Scripts
- Controle de direção de transferência de arquivo e tamanho de arquivo
- Fornece relatório completo de análise de comportamento de arquivos maliciosos
- Compartilhamento de inteligência global de ameaças, bloqueio de ameaças em tempo real
- Suporta somente o modo de detecção sem fazer upload de arquivos
- Configuração de lista de permissão / bloqueio de URL

Prevenção de C & C de Botnet

- Descubra o host botnet da intranet por monitoramento C & C conexões e bloqueando outras ameaças avançadas, como botnet e ransomware
- Atualiza regularmente os endereços do servidor de botnets
- Prevenção para C&C IP e domínio
- Suporta TCP, HTTP e DNS detecção de tráfego
- Permitir e bloquear a lista com base no endereço IP ou nome de domínio
- Suporta a detecção de sinkhole de DNS e tunelamento de DNS
- Suporta detecção DGA

Reputação de IP

- Identificar e filtrar o tráfego de riscos IPs, como hosts de botnet, spammers, Tor nodes, hosts violados e ataques de força bruta
- Registrando, descartando pacotes ou bloqueando para diferentes tipos de tráfego de risco IP
- Atualização do banco de dados de assinatura de reputação de IP regular

Decodificação de SSL

- Identificação de aplicação para tráfego SSL criptografado
- Habilitação de IPS para tráfego SSL criptografado
- Habilitação de AV para tráfego SSL criptografado
- Filtro de URL para tráfego SSL criptografado
- Lista de autorização de tráfego SSL criptografado
- Modo offload de proxy SSL
- Suporte à identificação de aplicativos, DLP, sandbox IPS, AV para tráfego descriptografado de proxy SSL de SMTPS / POP3S / IMAPS

Identificação e controle de endpoint

- Suporte para identificar IP de endpoint, quantidade de endpoints, tempo online, tempo offline e duração online
- Suporte a 10 sistemas operacionais, incluindo Windows, iOS, Android, etc.
- Suporte de consulta com base em IP, quantidade de ponto de extremidade, política de controle e status etc.
- Suporta a identificação da quantidade de terminais acessados na camada 3, registro e interferência no IP excedido
- Redirecionamento de exibição de página após operação de interferência personalizada
- Suporta a operações de bloqueio no IP excedido
- Identificação de usuário e controle de tráfego para serviços de desktop remoto do Windows Server

Segurança de Dados

- Controle de transferência de arquivos com base no tipo, tamanho e nome do arquivo
- Identificação de protocolo de arquivo, incluindo HTTP, FTP, SMTP, POP3 e SMB
- Assinatura de arquivo e identificação de sufixo para mais de 100 tipos de arquivo
- Filtragem de conteúdo para protocolos HTTP-GET, HTTP-POST, FTP e SMTP
- Identificação de IM e auditoria de comportamento de rede
- Filtre arquivos transmitidos por HTTPS usando proxy SSL e SMB

Recursos (Continua)

Controle de Aplicação

- Mais de 4 mil aplicações que podem ser filtradas por nome, categoria, subcategoria, tecnologia e risco
- Cada aplicação contém uma descrição, fatores de risco, dependências, portas típicas usadas e URLs para referência adicional
- Ações: bloquear, redefinir sessão, monitorar, formatar tráfego
- Identifica e controla aplicações de nuvem na nuvem
- Oferece monitoramento multidimensional e estatísticas de aplicações de nuvem, incluindo categoria e características de risco

Qualidade do Serviço (QoS)

- Túneis de largura de banda máxima/garantida ou com base em IP/usuário
- Alocação de túnel baseada em domínio de segurança, interface, endereço, usuário/grupo de usuários, servidor/grupo de servidores, aplicação/grupo de aplicações, TOS, VLAN
- Largura de banda alocada por tempo, prioridade ou compartilhamento de largura de banda equivalente
- Suporte a Tipo de Serviço (TOS) e Serviços Diferenciados (DiffServ)
- Alocação prioritária da largura de banda restante
- Conexões simultâneas máximas por IP
- Alocação de largura de banda baseada na categoria de URL
- Largura de banda limite atrasando o acesso para o usuário ou IP
- Limpeza de expiração automática e limpeza manual do tráfego usado pelo usuário

Balanceamento de Carga de Servidor

- Ponderação de hashing, least-connection e round-robin
- Proteção de sessão, persistência de sessão e monitoramento de status de sessão
- Verificação de integridade de servidor, monitoramento de sessão e proteção de sessão

Balanceamento de Carga de Link

- Balanceamento de carga de link bidirecional
- Balanceamento de carga de link de saída: roteamento baseado em política, incluindo ECMP, roteamento de tempo, ponderado e integrado de ISP; detecção ativa e passiva da qualidade do link em tempo real e seleção da melhor rota
- O balanceamento de carga de link de entrada suporta SmartDNS e detecção dinâmica
- Comutação automática de link baseada em largura de banda, latência, jitter, conectividade, aplicação etc.
- Inspeção de integridade de link com ARP, PING e DNS

VPN

- VPN IPsec
 - Modo IPsec Fase 1: modo de proteção agressiva e ID principal
 - Opções de aceitação peer: qualquer ID, ID específico, ID em grupo de usuário discado
 - Suporta IKEv1 e IKEv2 (RFC 4306)
 - Método de autenticação: certificada e chave pré-com partilhada
 - Suporte a configuração de modo IKE (como servidor ou cliente)

- DHCP via IPsec
- Expiração de chave de criptografia IKE configurável, NAT transversal mantém a frequência viva
- Criptografia de proposta Fase 1/Fase 2: DES, 3DES, AES128, AES192, AES256
- Autenticação de proposta Fase 1/Fase 2: MD5, SHA1, SHA256, SHA384, SHA512
- IKEv1 suporta grupo DH 1,2,5,19,20,21,24
- IKEv2 suporta grupo DH 1,2,5,14,15,16,19,20,21,24
- XAuth como modo servidor e para usuários discados
- Detecção dead peer
- Detecção de replay
- Autokey keep-alive para Fase 2 SA
- Suporte a domínio VPN IPsec: permite diversos logins SSL VPN personalizados associados a grupos de usuários (caminhos de URL, design)
- Opções de configuração de VPN IPsec: baseada em rota ou política
- Modos de implementação de VPN IPsec: gateway-to-gateway, full mesh, hub-and-spoke, túnel redundante, terminação de VPN em modo transparente
- O login único impede logins simultâneos com o mesmo nome de usuário
- Limitação de usuários simultâneos de portal SSL
- O módulo de encaminhamento de porta SSL VPN criptografa dados do cliente e envia os dados para o servidor da aplicação
- Suporta clientes que executam iOS, Android e Windows XP/Vista, incluindo SO Windows de 64 bits
- Verificação de integridade de host e verificação de SO antes de conexões de túnel SSL
- Verificação de host MAC por portal
- Opção de limpeza de cache antes de finalização de sessão SSL VPN
- Modo L2TP cliente e servidor, L2TP sobre IPsec e GRE sobre IPsec
- Visualiza e gerencia conexões IPsec e SSL VPN
- PnPVPN
- VTEP para túnel unicast estático VXLAN

IPv6

- Gerenciamento sobre IPv6, registro de IPv6 e HA
- Tunelamento IPv6: DNS64 / NAT64, IPv6 ISATAP, IPv6 GRE, IPv6 sobre IPv4 GRE
- Protocolos de roteamento IPv6, roteamento estático, roteamento de política, ISIS, RIPng, OSPFv3 e BGP4+
- IPS, Identificação de Aplicação, antivírus, controle de acesso, contra-ataque ND, iQoS
- Suporte a jumbo frame IPv6
- Suporte a IPv6 Radius
- Suporte IPv6 nos seguintes ALGs: TFTP, FTP, RSH, HTTP, SIP
- Suporte IPv6 em iQoS distribuído
- Rastrear detecção de endereço

VSYS (disponível apenas em modelos de montagem em rack)

- Alocação de recursos de sistema para cada VSYS
- Virtualização de CPU
- Firewall de suporte a VSYS não raiz, VPN IPsec, VPN SSL, IPS, filtragem de URL, monitoramento de aplicativo, reputação de IP, AV, QoS
- Monitoramento e estatísticas de VSYS, Identificação de Aplicação, reputação de IP, AV, QoS

Alta Disponibilidade

- Interfaces heartbeat redundantes
- Modo ativo / passivo e par
- Sincronização de sessão standalone
- Interface reservada de gerenciamento de HA
- Failover:
 - Monitoramento de porta e link local e remoto
 - Failover com estado
 - Failover sub-secundário
 - Notificação de falha
- Opções de implementação:
 - HA com agregação de link
 - HA mash completo
 - HA com dispersão geográfica
- Duas portas de link de dados HA

Alta Disponibilidade em Twin-mode (disponível apenas nos modelos A3000 e acima)

- Modo de alta disponibilidade entre vários dispositivos
- Vários modos de implementação de Alta Disponibilidade
- Sincronização de configuração e de sessão entre vários dispositivos

Identidade de Usuário e Dispositivo

- Banco de dados local de usuários
- Autenticação de usuário remoto: TACACS+, LDAP, Radius, Diretório Ativo
- Single-sign-on: Windows AD
- Autenticação de dois fatores: suporte a terceiros, servidor de token integrado com físico e SMS
- Políticas baseadas em usuário e dispositivo
- Sincronização de grupo de usuários baseada no AD e em LDAP
- Suporte a 802.1X, Proxy SSO
- WebAuth: personalização de página, prevenção de crack de força, suporte IPv6
- Autenticação baseada em interface
- ADSSO sem agente (AD Polling)
- Usa sincronização de autenticação baseada em monitor de SSO
- Suporta autenticação de usuário baseada em IP e MAC
- O servidor Radius emite política de segurança do usuário via mensagem CoA

Administração

- Acesso de gerenciamento: HTTP/HTTPS, SSH, telnet, console
- Gerenciamento central: Hillstone Security Manager (HSM), APIs de serviço da Web
- Integração de sistema: SNMP, syslog, parcerias de aliança
- Implementação rápida: instalação automática via USB, execução de script local e remoto
- Status de painel dinâmico em tempo real e widgets de monitoramento detalhado
- Suporte a idioma: Inglês

Logs e Relatórios

- Instalações de registro: armazenamento local; até 6 meses de armazenamento de log com armazenamento de expansão (disco rígido SSD), servidor syslog, Hillstone HSM ou HSA
- Log criptografado e integridade de log com carregamento de log em lote HSA programado

Recursos (Continua)

- Log confiável usando opção TCP (RFC 3195)
- Logs detalhados de tráfego: encaminhados, sessões violadas, tráfego local, pacotes inválidos, URL etc.
- Logs abrangentes de eventos: auditoria de atividade de sistema e administrativa, roteamento e rede, VPN, autenticações de usuário, eventos relacionados a Wi-Fi
- Opção de resolução de nome de porta IP e de serviço
- Opção de formato de log de tráfego breve
- Três relatórios predefinidos: relatórios de Segurança, Fluxo e rede
- Relatórios definidos pelo usuário
- Os relatórios podem ser exportados em PDF por Email e FTP

Estatísticas e Monitoramento

- Aplicativo, URL, estatística e monitoramento de eventos de ameaça
- Estatística e análise de tráfego em tempo real
- Informações do sistema, como sessão simultânea, CPU, memória e temperatura
- Estatística de tráfego iQOS e monitoramento, monitoramento de status de link
- Suporte a coleta de informações de tráfego e encaminhamento via Netflow (v9.0)





CloudView

- Monitoramento de segurança baseada em nuvem
- Acesso 24x7 pela Web ou aplicativo móvel
- Status de dispositivo, monitoramento de tráfego e ameaça
- Retenção e relatório de log baseado na nuvem

Especificações do Produto

	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

Especificações do Produto (Contínua)

	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

Opções de Módulo

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)

OBSERVAÇÕES:

(1) Os dados de transferência do firewall são obtidos no tráfego UDP com tamanho de pacote de 1518 bytes. A taxa de transferência do firewall para A3700 e A3800 pode ser aumentada de 20 Gbps para 40 Gbps por meio do módulo de expansão IOC-A-4SFP+ adicional;

(2) os dados de capacidade NGFW são obtidos em tráfego HTTP de 64 Kbytes com controle de aplicação e IPS habilitados;

(3) os dados de capacidade de proteção de ameaça são obtidos em tráfego HTTP de 64 Kbytes com controle de aplicação, IPS, AV, filtro de URL, ABD e ATD habilitados;

(4) O máximo de sessões simultâneas é obtido no tráfego HTTP;

(5) Novas sessões são obtidas em tráfego HTTP;

(6) os dados de capacidade IPS são obtidos com detecção de tráfego;

(7) os dados de capacidade AV são obtidos em tráfego HTTP com anexação de arquivo.

A menos que especificado de outra forma, todos os recursos, funções e o desempenho são baseados no StoneOS5.5R8. Os resultados podem variar dependendo da versão e implementação do StoneOS®.