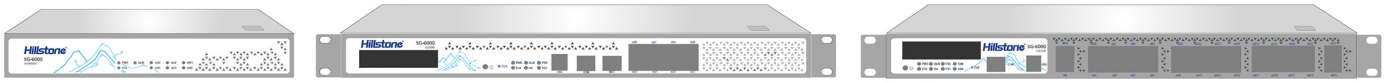
Hillstone A-Series
Next-Generation Firewall



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. Como parte da solução ZTNA, o NGFW da Série-A controla, de maneira granular, o acesso à aplicação com a eliminação de confiança implícita e verificação contínua. 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 desktop, têm um grande armazenamento interno e possuem opções de expansão para até 2 TB de armazenamento em disco. 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 para criação de políticas baseadas em serviço em aplicação
- 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)

Antivirus
- 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
- Defesa contra ataque Flood, incluindo ICMP flood, UDP flood, DNS query flood, DNS query flood recursivo, DNS reply flood, SYN flood
- Defesa contra ARP spoofing e ND spoofing
- Defesa contra Scan e Spoof, incluindo IP address spoof, IP address sweep, scan de porta
- Defesa contra DoS/DDoS, incluindo ataque ping of death, teardrop, IP fragment, IP option, Smurf ou Fragile, Land, pacote grande de ICMP, WinNuke
- 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(1)
- 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 ameaça 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
- Proxy SSL suporta lista de permissão IP e lista de permissão pré-definida
- Suporta TLSv1.2 e TLSv1.3
- 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
- Filtro de conteúdo para palavras-chave

Recursos (Contínua)

pré-definidas e conteúdo de arquivos
- Identificação de IM e auditoria de comportamento de rede
- Filtre arquivos transmitidos por HTTPS usando proxy SSL e SMB

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), Serviços Diferenciados (DiffServ) e Classe de Tráfego (traffic-class)
- 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 config urável, 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)
- Guia de Configuração de suporte a VPN IPSec. Opções de configuração incluem: baseada em rota e em 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 rodam iOS, Android, Microsoft Windows, MacOS e Linux
- 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 Log IPv6, Alta Disponibilidade (HA e HA modo peer), twin-mode ativo-ativo (AA) e ativo-passivo (AP)
- 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+
- Suporte a IPv6 no balanceador de link (LLB)
- IPS, Identificação de Aplicação, Filtro de URL, Anti-vírus, Controle de Acesso, Ataque Defesa ND, iQoS, VPN SSL
- Suporte a jumbo frame IPv6
- Suporta IPv6 Radius e SSO-radius
- IPv6 é suportado na lista de permissão do Active Directory
- Suporte IPv6 nos seguintes ALGs: TFTP, FTP, RSH, HTTP, SIP, SQLNETv2, RTSP, MSRPC, SUNRPC
- 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 heatbeat redundantes
- Ativo / passivo e modo 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

Recursos (Contínua)

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
- Autenticação de administrador: Active Directory e LDAP

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
- 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
- Suporta auditoria de configuração de políticas

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

Segurança de dispositivos IoT
- Identificar dispositivos IoT, como Câmeras IP e Gravadores de Vídeo em Rede
- Suporte à consulta de resultados de monitoramento com base nas condições de filtragem, incluindo tipo de dispositivo, endereço IP, status etc
- Suportar whitelists personalizados

Especificações do Produto

	SG-6000-A200	SG-6000-A200W	SG-6000-A1000	SG-6000-A1100	SG-6000-A2000	SG-6000-A2600
						
Firewall Throughput [2]	1 Gbps	1 Gbps	4 Gbps	5 Gbps	5 Gbps	5 Gbps
NGFW Throughput [3]	400 Mbps	400 Mbps	1.5 Gbps	1.7 Gbps	1.7 Gbps	2.5 Gbps
Threat Protection Throughput [4]	200 Mbps	200 Mbps	800 Mbps	800 Mbps	800 Mbps	1.8 Gbps
Maximum Concurrent Sessions [5]	300,000	300,000	300,000	300,000	1 Million	1.2 Million
New Sessions/s [6]	15,000	15,000	48,000	48,000	48,000	120,000
IPS Throughput [7]	610 Mbps	610 Mbps	3.4 Gbps	3.7 Gbps	3.2 Gbps	4.5 Gbps
AV Throughput [8]	550 Mbps	550 Mbps	1.8 Gbps	2.0 Gbps	2.0 Gbps	3.7 Gbps
IPsec VPN Throughput [9]	0.62 Gbps	0.62 Gbps	2.5 Gbps	2.7 Gbps	2.7 Gbps	3 Gbps
SSL Proxy Throughput [10]	15 Mbps	15 Mbps	250 Mbps	250 Mbps	250 Mbps	750 Mbps
Virtual Systems (Default/Max)	N/A	N/A	N/A	N/A	1/5	1/5
Firewall Policy Number	4000	4000	4,000	4,000	8,000	12,000
SSL VPN Users (Default/Max)	8/128	8/128	8/128	8/128	8/1,000	8/2,000
IPsec Tunnel Number	2,000	2,000	2,000	2,000	4,000	6,000
Management Ports	1 × Console Port, 1 × USB 2.0 Port	1 × Console Port, 1 × USB 2.0 Port	1 × Console Port, 2 × USB3.0 Ports	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45)
Fixed I/O Ports [11]	1×SFP, 5×GE	1×SFP, 5×GE	4 × GE	8 × GE (including 1 bypass pair)	8 × GE (including 1 bypass pair)	8 × GE (including 1 bypass pair)
Wi-Fi	N/A	IEEE802.11a/b/g/n/ac	N/A	N/A	N/A	N/A
Available Slots for Expansion Modules	N/A	N/A	N/A	N/A	N/A	N/A
Expansion Module Option	N/A	N/A	N/A	N/A	N/A	N/A
Twin-mode HA	N/A	N/A	N/A	N/A	N/A	N/A
Local Storage	4 GB	4 GB	8 GB	8 GB	8 GB	8 GB
Expansion Storage Options	N/A	N/A	256 GB SSD	256 GB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD
Power Specification	14W, Single AC (default)	14W, Single AC (default)	30W, Single AC	30W, 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	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	Desktop	Desktop	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	180 × 110 × 28	180 × 110 × 28	270 × 160 × 44	270 × 160 × 44	436 × 320 × 44	436 × 320 × 44
Dimensions (W × D × H, inches)	7.1 × 4.3 × 1.1	7.1 × 4.3 × 1.1	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	2.2 lb (0.6 kg)	2.2 lb (0.6 kg)	3.1 lb (1.4 kg)	3.1 lb (1.4 kg)	8.6 lb (3.9 kg)	8.6 lb (3.9 kg)
Working 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)	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	10-95% non-condensing	10-95% non-condensing

Especificações do Produto (Contínua)

	SG-6000-A2700	SG-6000-A2800	SG-6000-A3000	SG-6000-A3600	SG-6000-A3700	SG-6000-A3800
						
Firewall Throughput [2]	10 Gbps	16 Gbps	20 Gbps	20 Gbps	20 / 40 Gbps	20 / 40 Gbps
NGFW Throughput [3]	3 Gbps	4.5 Gbps	5.5 Gbps	5.5 Gbps	6 Gbps	12 Gbps
Threat Protection Throughput [4]	2 Gbps	2.8 Gbps	3 Gbps	3 Gbps	3.1 Gbps	6 Gbps
Maximum Concurrent Sessions [5]	1.5 Million	1.8 Million	2 Million	3 Million	6 Million	8 Million
New Sessions/s [6]	130,000	130,000	140,000	140,000	140,000	310,000
IPS Throughput [7]	5 Gbps	8 Gbps	10 Gbps	10 Gbps	10 Gbps	20 Gbps
AV Throughput [8]	4.2 Gbps	4.2 Gbps	4.9 Gbps	5.0 Gbps	5.2 Gbps	9.4 Gbps
IPsec VPN Throughput [9]	5 Gbps	5.5 Gbps	6 Gbps	6 Gbps	6.5 Gbps	12 Gbps
SSL Proxy Throughput [10]	800 Mbps	800 Mbps	950 Mbps	950 Mbps	950 Mbps	2 Gbps
Virtual Systems (Default/Max)	1/5	1/5	1/50	1/100	1/250	1/250
SSL VPN Users (Default/Max)	8/4,000	8/4,000	8/4,000	8/8,000	8/10,000	8/10,000
IPsec Tunnel Number	6,000	6,000	8,000	10,000	20,000	20,000
Firewall Policy Number	12,000	12,000	20,000	20,000	20,000	40,000
Management Ports	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)
Fixed I/O Ports [11]	2 × SFP+, 8 × SFP, 8 × GE	2 × SFP+, 8 × SFP, 8 × GE	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)
Wi-Fi	N/A	N/A	N/A	N/A	N/A	N/A
Available Slots for Expansion Modules	N/A	N/A	N/A	N/A	1	1
Expansion Module Option	N/A	N/A	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	N/A	N/A	Yes	Yes	Yes	Yes
Local Storage	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB
Expansion Storage Options	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD
Power Specification	50W, Single AC (default), Dual AC (optional)	50W, Single AC (default), Dual AC (optional)	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 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 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	AC 100-240 V 50/60 Hz DC -36~-72 V
Form Factor	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	440 x 320 x 44	440 x 320 x 44	436 × 437 × 44	436 × 437 × 44	436 × 437 × 44	436 × 437 × 44
Dimensions (W × D × H, inches)	17.3 x 12.6 x 1.7	17.3 x 12.6 x 1.7	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	9 lb (4.1 kg)	9 lb (4.1 kg)	13.2 lb (6 kg)	13.2 lb (6 kg)	13.4 lb (6.1 kg)	15 lb (6.8 kg)
Working 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)	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	10-95% non-condensing	10-95% non-condensing

Especificações do Produto (Contínua)

	SG-6000-A5100	SG-6000-A5200	SG-6000-A5500	SG-6000-A5600	SG-6000-A5800
					
Firewall Throughput [2]	25/50 Gbps	32/65 Gbps	40/80 Gbps	60/85 Gbps	80/95 Gbps
NGFW Throughput [3]	9 Gbps	20 Gbps	25 Gbps	29 Gbps	32 Gbps
Threat Protection Throughput [4]	6 Gbps	12 Gbps	15 Gbps	18 Gbps	20 Gbps
Maximum Concurrent Sessions [5]	8 Million	12 Million	13 Million	20 Million	25 Million
New Sessions/s [6]	350,000	400,000	500,000	800,000	930,000
IPS Throughput [7]	20/25 Gbps	20/35 Gbps	25/40 Gbps	35/60 Gbps	45/75 Gbps
AV Throughput [8]	12 Gbps	12 Gbps	15 Gbps	20 Gbps	25 Gbps
IPsec VPN Throughput [9]	15 Gbps	20 Gbps	28 Gbps	36 Gbps	45 Gbps
SSL Proxy Throughput [10]	3 Gbps	5 Gbps	5 Gbps	8.5 Gbps	8.5 Gbps
Virtual Systems (Default/Max)	1/250	1/250	1/250	1/500	1/500
SSL VPN Users (Default/Max)	8/10,000	8/10,000	8/10,000	8/10,000	8/10,000
IPsec Tunnel Number	20,000	20,000	20,000	20,000	20,000
Firewall Policy Number	40,000	40,000	60,000	60,000	80,000
Management Ports	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 2 × HA ports (SFP+)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 2 × HA ports (SFP+)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 2 × HA ports (SFP+)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA port (SFP)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA port (SFP)
Fixed I/O Ports [11]	6 × SFP+, 16 × SFP, 8 × GE (including 2 bypass pairs)	6 × SFP+, 16× SFP, 8× GE (including 2 bypass pairs)	6 × SFP+, 16× SFP, 8× GE (including 2 bypass pairs)	2 × QSFP+, 16 × SFP+, 8 × GE (including 4 bypass pairs)	2 × QSFP+, 16 × SFP+, 8 × GE (including 4 bypass pairs)
Wi-Fi	N/A	N/A	N/A	N/A	N/A
Available Slots for Expansion Modules	1	1	1	1	1
Expansion Module Option	IOC-A-4SFP+, IOC-A-2QSFP+, IOC-A-2MM-BE, IOC-A-2SM-BE	IOC-A-4SFP+, IOC-A-2QSFP+, IOC-A-2MM-BE, IOC-A-2SM-BE	IOC-A-4SFP+, IOC-A-2QSFP+, IOC-A-2MM-BE, IOC-A-2SM-BE	IOC-A-4SFP+, IOC-A-2QSFP+, IOC-A-2MM-BE, IOC-A-2SM-BE	IOC-A-4SFP+, IOC-A-2QSFP+, IOC-A-2MM-BE, IOC-A-2SM-BE
Twin-mode HA	Yes	Yes	Yes	Yes	Yes
Local Storage	64 GB	64 GB	64 GB	64 GB	64 GB
Expansion Storage Options	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD
Power Specification	280W, Dual AC (default), Dual DC (optional)	280W, Dual AC (default), Dual DC (optional)	280W, Dual AC (default), Dual DC (optional)	300W, Dual AC (default), Dual DC (optional)	300W, Dual AC (default), Dual DC (optional)
Power Supply	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V
Form Factor	Rackmount, 1U	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	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	17.2 × 17.2 × 1.7
Weight	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)
Working 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)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	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	IOC-A-2QSFP+
				
Names	4SFP+ Expansion Module	4SFP Multi-mode Bypass Expansion Module	4SFP Single-mode Bypass Expansion Module	2QSFP+ Expansion Module
I/O Ports (11)	4 × SFP+, SFP+ module not included	4 × SFP, MM bypass (2 pairs of bypass ports)	4 × SFP, SM bypass (2 pairs of bypass ports)	2 × QSFP+
Dimension	1U	1U	1U	1U
Weight	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)

OBSERVAÇÕES:

(1) A funcionalidade de Anti-Spam não está disponível no SG-6000-A200 e SG-6000-A200W;

(2) Os dados de transferência do firewall são obtidos no tráfego UDP com tamanho de pacote de 1518 bytes. A performance de firewall do A3700 e A3800 pode ser aumentada de 20 Gbps para 40 Gbps com a adição do módulo de expansão IOC-A-4SFP+. O throughput de firewall para os A5100/A5200/A5500/A5600/A5800 pode ser aumentado para 50/65/80/85/95 Gbps, respectivamente, com a adição do módulo de expansão IOC-A-2QSFP+;

(3) os dados de capacidade NGFW são obtidos em tráfego HTTP de 64 Kbytes com controle de aplicação e IPS habilitados. O parâmetro de throughput de NGFW do A5100 é testado com a versão StoneOS5.5R8;

(4) 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. O parâmetro de throughput de proteção contra ameaças do A5100 é testado com a versão StoneOS5.5R8;

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

(6) Novas sessões são obtidas em tráfego HTTP;

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

(8) os dados de capacidade AV são obtidos em tráfego HTTP com anexação de arquivo;

(9) os dados de capacidade IPSec são obtidos na configuração Preshare Key AES256+SHA-1 e em pacotes de 1.400 bytes;

(10) Dados de throughput de Proxy SSL são obtidos usando AES128-GCM-SHA256 com todas as regras de IPS ativas;

(11) Portas SFP+ suportam módulo óptico SFP+ 10Gbps, módulo óptico SFP 1000Mbps e módulo de cobre SFP 1000Mbps; Portas QSFP+ suportam módulo 40GE 1×40Gbps e módulos 4×10GE 4×10Gbps.

A menos que especificado de outra forma, todos os recursos, funções e o desempenho são baseados no StoneOS5.5R9. Os resultados podem variar dependendo da versão e implementação do StoneOS®.

Version: EX-08.01-NGFW-A-Series-5.5R9-0722-PT-01