

# Hillstone S-Series Network Intrusion Prevention System (NIPS)



Na medida em que o cenário de ameaças avança agressivamente, um crescente número de tecnologias de proteção de rede tem surgido rapidamente. Dentre essas várias tecnologias, o Intrusion Prevention System (IPS) continua sendo uma das soluções mais amplamente implementadas, independentemente da plataforma ou fator de forma.

O dispositivo Hillstone Network-based IPS (NIPS) opera em linha e em velocidade máxima, fazendo inspeção profunda de pacote e compondo inspeção de todo o tráfego da rede. Ele também aplica regras com base em diversas metodologias, incluindo análise de protocolo anômalo e análise de assinatura, para bloquear ameaças. O Hillstone NIPS pode ser implementado na rede para inspecionar o tráfego deixado não detectado por soluções de perímetro, e é uma parte integrante dos sistemas de segurança de rede pelo seu alto desempenho, não comprometimento, recursos de proteção da melhor qualidade e cenários de implementação amplos e flexíveis.

## Destaques do Produto

### **Proteção sem Comparação Contra Ameaças sem comprometimento de desempenho**

A plataforma Hillstone NIPS tem o mais abrangente mecanismo de inspeção de alto desempenho, combinado com a parceria de assinatura da melhor qualidade e com parceiros líderes de tecnologia, oferecendo aos clientes a maior taxa de detecção de ameaças com o mais baixo custo total de propriedade (TCO). O mecanismo Hillstone NIPS tem 99,6% de taxa de bloqueio de explorações estáticas e 98,325% de taxa de bloqueio de explorações ao vivo (reportado pela NSS Labs).

A plataforma Hillstone NIPS oferece alta capacidade, baixa latência e máxima disponibilidade para manter eficientes operações de segurança sem comprometer o desempenho da rede. O NIPS com-

bina análise de protocolo, reputação de ameaça e outros recursos, que fornecem proteção contra ameaça da Camada 2 à Camada 7, incluindo ataque ARP, ataque Dos/DDoS, protocolos anormais, URLs maliciosos, malwares e ataques web.

### **Relatórios Granulares com Pontos de Vista Dirigidos ao Usuário**

O Hillstone NIPS oferece abrangente visibilidade baseada no protocolo, aplicação, usuário e conteúdo. Ele pode identificar mais de 4,000 aplicações, incluindo centenas de aplicativos móveis e na nuvem. Por reunir diversas fontes, o sistema pode identificar informação contextual para tomar as devidas decisões de bloqueio. Com uma função granular e robusta de relatórios, ele oferece visibilidade de diferentes visualizações:

## Destaques do Produto (Continuação)

- Modelos únicos, com base na sua função: administrador de sistema de negócio, administrador de segurança ou CIO ou executivo.
- Conteúdo de Ameaça Organizado - se um risco de sistema ou de segurança, ameaça de rede ou visualização de tráfego - para ajudá-lo a compreender claramente o risco e tomar a decisão certa.

## Facilidade de Implementação e Gerenciamento Centralizado

Implementar e gerenciar o Hillstone NIPS é simples, com custos gerais mínimos. Ele pode ser implementado nos seguintes modos para satisfazer requisitos de segurança e garantir conectividade

## Recursos

### 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 e revisão com base em filtros: 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

### Análise de Correlação de Ameaças

- Correlação entre ameaças desconhecidas, comportamento anormal e comportamento do aplicativo para descobrir ameaças ou ataques em potencial
- Regras de correlação multidimensionais, atualização diária automática na nuvem

### Detecção Avançada de Ameaças

- Detecção avançada de malware baseada em comportamento
- Detecção de mais de 2.000 famílias de malware conhecidas e desconhecidas, incluindo vírus, worm, cavalo de Troia, spyware, overflow, etc.
- Atualização online e em tempo real de banco de dados de modelo de comportamento de malware

### Detecção de Comportamento Anormal

- Modelagem de comportamento com base em tráfego de linha de base L3-L7 para revelar comportamento anômalo de rede, como varredura HTTP, Spider, SPAM, senha fraca de SSH/FTP e spyware
- Detecção de mais de 2.000 famílias de malware conhecidas e desconhecidas, incluindo vírus, worm, cavalo de Troia, overflow, etc.
- Suporta inspeção de tráfego de tunelamento criptografado para aplicações desconhecidas
- Atualização online em tempo real do banco de dados de modelo de comportamento anormal

### Antivírus

- Atualizações de assinatura push ou pull manual e automática
- Antivírus baseado em fluxo: os protocolos incluem HTTP/HTTPS, SMTP, POP3, IMAP, FTP / SFTP e SMB
- Varredura de vírus em arquivo compactado

ideal de rede:

- Proteção ativa (modo de prevenção de intrusão), monitoramento e bloqueio em tempo real.
- Detecção passiva (modo de detecção de intrusão), monitoramento e alerta em tempo real.

O Hillstone NIPS pode ser gerenciado pela Hillstone Security Management Platform (HSM). Os administradores podem registrar, monitorar e atualizar de forma centralizada dispositivos NIPS implementados em diferentes filiais ou localizações, com uma política unificada de gerenciamento na rede para eficiência máxima.

### Defesa de Ataques

- Defesa de ataques com protocolo anormais
- Anti-DoS / DDoS, incluindo SYN Flood, defesa de inundações de consultas DNS
- Defesa de ataques ARP

### Filtro de URL

- Inspeção de filtragem Web com base no fluxo
- Filtragem Web definida manualmente com base na URL, conteúdo da Web e cabeçalho MIME
- Filtragem Web dinâmica com base em dados de categorização em tempo real, com base na nuvem: mais de 140 milhões de URLs com 64 categorias (8 das quais relacionadas à segurança)
- Recursos adicionais da filtragem da web:
  - Filtragem de Java Applets, ActiveX ou cookies
  - Bloqueio de postagem HTTP
  - Registro de palavras-chave de pesquisa
  - Por privacidade, conexões criptografadas isentas de verificação em determinadas categorias
- Cancelamento do perfil Web de filtragem: permite que o administrador atribua temporariamente diferentes perfis de usuário / grupo / IP
- Filtro Web para categorias locais e cancelamento de categorias qualificadas
- Lista de permissão / bloqueio de suporte
- Alarme personalizável

### Anti-spam

- Classificação e prevenção de spam em tempo real
- Spam confirmado, spam suspeito, spam em massa, volume válido
- Proteção Independentemente do idioma, formato ou conteúdo da mensagem
- Admite protocolos de email SMTP e POP3
- Detecção de entrada e saída
- As listas brancas permitem e-mails de domínios / endereços de e-mails confiáveis
- As listas negras são definidas pelo usuário

### Sandbox de Nuvem

- Carregamento de arquivos maliciosos em sandbox de nuvem para análise, incluindo tráfego HTTPS criptografado
- Protocolos de suporte que incluem HTTP / HTTPS, POP3, IMAP, SMTP e FTP
- Tipos de arquivos suportados, incluindo PE, ZIP, RAR, Office, PDF, APK, JAR e SWF
- Endereço de transferência de arquivo e controle de tamanho de arquivo
- Fornece relatório completo de análise de comportamento de arquivos maliciosos
- Intercâmbio global de inteligência contra ameaças, bloqueio de ameaças em tempo real

## Recursos (Continuação)

### Botnet com prevenção CyC

- Descobre a intranet botnet host através de controles das conexões CyC e bloqueia outras ameaças avançadas como botnet e ransomware
- Atualiza regularmente os endereços do servidor botnet
- Prevenção para CyC IP e domínios
- Suporte para a detecção de tráfego TCP, HTTP e DNS
- Listas brancas de IP e domínios

### Reputação das IP

- Identifica e filtra o tráfego de risco IP, como host de botnet, spammers, TOR, hosts violados e ataques de força bruta
- Registros, queda de pacotes ou bloqueio para diferentes tipos de risco no tráfego IP
- Atualização constante do banco de dados IP por reputação e assinaturas

### 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, monitorar
- Oferece monitoramento multidimensional e estatísticas de aplicações de nuvem, incluindo categoria e características de risco
- Suporta aplicativo criptografado

### Qualidade de Serviço (QoS)

- Número máximo de túneis / largura de banda garantida ou por IP / usuário
- Atribuição de túnel com base no domínio de segurança, interface, endereço, usuário/grupo, servidor/grupo de servidores, aplicativo/ grupo de aplicativos, TOS, VLAN
- Largura de banda alocada por tempo, prioridade ou distribuição equitativa da largura de banda
- Tipo de Serviço (TOS) e suporte para serviços diferenciados (DiffServ)
- Atribuição de prioridades de largura de banda restantes
- Número máximo de conexões simultâneas por IP
- Alocação de largura de banda de acordo com a categoria de URL
- Limite de largura de banda atrasando o acesso do usuário ou IP

### IPv6

- Gerenciamento sobre IPv6, registro de IPv6 e HA
- Túneis IPv6, DNS64 / NAT64 etc.
- Protocolos de roteamento IPv6, roteamento estático, roteamento por política, ISIS, RIPng, OSPFv3 e BGP4+
- IPS, identificação de aplicativos, controle de acesso, defesa de ataques ND

### VSYS

- Alocação de recursos do sistema para cada VSYS
- Virtualização de CPU
- VSYS não raiz oferece suporte a IPS, filtragem de URL, política, QoS, etc.
- Monitoramento e estatísticas VSYS
- Suporta backup de todas as configurações VSYS de uma vez

### SSL Proxy

- Descarregamento de SSL: descrição de tráfego SSL
- SSL requerido / isento: tráfego SSL permitido ou bloqueado com base nas regras da política sem descrição

### Análise e controle de tráfego flexível

- Suporta 3 modos de operação: Rota / NAT (camada 3), Transparente (camada 2) com interface de desvio opcional e modo TAP (Modo IDS) com Integração de Firewall Hillstone
- Análise e controle de tráfego com base em regras de política por zona de origem / destino, endereço IP de origem / destino, usuários, serviço ou aplicativos

### Alta Disponibilidade

- Interfaces heartbeat redundantes
- Modo ativo/passivo e de pares
- 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

### Administração Visível

- Acesso de gerenciamento: HTTP/HTTPS, SSH, telnet, console
- Gerenciamento central: Hillstone Security Manager (HSM), APIs de serviço da Web
- Autenticação de dois fatores: nome de usuário/senha, arquivo de certificado HTTPS
- 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
- Gerenciamento de dispositivos de armazenamento: personalização e alarme de limite de espaço de armazenamento, sobreposição de dados antigos, parar registro.
- Suporte a idioma: Inglês

### Logs e relatórios

- Instalações de registro: vários servidores syslog e várias plataformas Hillstone Security Audit (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
- Relatórios granulares com visualizações personalizadas para o usuário
  - Gerenciamento HA/visualização de nível C
  - Visualização de Proprietário de Sistema de Negócio
  - Visualização de Administrador de Segurança de Rede

### Estatísticas e monitoramento

- Estatísticas de eventos de ameaças e monitoramento de aplicativos e URL
- Análise e estatísticas de tráfego em tempo real
- Informações do sistema, como sessão simultânea, CPU, memória e temperatura
- Estatísticas e monitoramento do tráfego iQoS, monitoramento do status de links
- Suporte para a coleta de informações de tráfego e encaminhamento via Netflow (v9.0)
- Serviço de inteligência de ameaças com base na nuvem
- Distribuição geográfica de ataques de rede externa

### CloudView

- Monitoramento de segurança baseado em nuvem
- Acesso 24/7 a partir da web ou de um aplicativo móvel
- Status do dispositivo, tráfego e monitoramento de ameaças
- Retenção e geração de relatórios de registros baseados na nuvem

## Especificações do Produto

|   | S600                                | S1060                               | S1560                               | S2160  | S2660  | S3560  | S3860  | S5560  |
|---|-------------------------------------|-------------------------------------|-------------------------------------|--|--|--|--|--|
| <b>IPS Throughput</b> <sup>(1)</sup>  | 1 Gbps                              | 3 Gbps                              | 4 Gbps                              | 10 Gbps  | 14 Gbps  | 16 Gbps  | 20 Gbps  | 50 Gbps  |
| <b>Maximum Concurrent Connections, TCP (Standard/with AEL)</b> <sup>(2)</sup> | 1 Million / 2 Million               | 1 Million / 2 Million               | 1 Million / 2 Million               | 2 Million / 4 Million  | 2 Million / 4 Million  | 4 Million / 8 Million  | 4 Million / 8 Million  | 8 Million / 10 Million   |
| <b>New Connections per Second, TCP</b> <sup>(3)</sup>                         | 9,000                               | 35,000                              | 41,000                              | 92,000   | 120,000  | 150,000  | 200,000  | 485,000  |
| <b>Stoneshield</b>  | N/A                                 | N/A                                 | Yes                                 | N/A  | Yes  | N/A  | Yes  | Yes  |
| <b>Virtual Systems (Default/Max)</b>  | 1/5                                 | 1/5                                 | 1/5                                 | 1/5  | 1/5  | 1/10   | 1/10   | 1/100  |
| <b>Storage</b>  | 1T                                  | 1T                                  | 1T                                  | 1T   | 1T   | 1T   | 1T   | 1T   |
| <b>Form Factor</b>  | 1U                                  | 1U                                  | 1U                                  | 1U   | 1U   | 2U   | 2U   | 2U   |
| <b>Management Ports</b>   | 2 x USB Port, 1 x Console Port      | 2 x USB Port, 1 x Console Port      | 2 x USB Port, 1 x Console Port      | 2 x USB Port, 2 x MGT, 1 x Console Port  | 2 x USB Port, 2 x MGT, 1 x Console Port  | 2 x USB Port, 2 x MGT, 1 x Console Port  | 2 x USB Port, 2 x MGT, 1 x Console Port  | 2 x USB Port, 2 x MGT, 1 x Console Port  |
| <b>Fixed I/O Ports</b>  | 4 x GE                              | 4 x GE                              | 4 x GE                              | 4 x GE   | 4 x GE   | 6 x GE   | 6 x GE   | N/A  |
| <b>Available Slots for Expansion Modules</b>                                  | 1 x Generic Slot                    | 1 x Generic Slot                    | 1 x Generic Slot                    | 2 x Generic Slot   | 2 x Generic Slot   | 2 x Generic Slot   | 2 x Generic Slot   | 4 x Generic Slot   |
| <b>Expansion Module Option</b>  | IOC-S-4GE-B-L, IOC-S-4SFP-L         | IOC-S-4GE-B-L, IOC-S-4SFP-L         | IOC-S-4GE-B-L, IOC-S-4SFP-L         | IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-4SFP-B, IOC-S-2SFP+, IOC-S-2SFP+B, IOC-S-4SFP+, IOC-S-4SFP+B | IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-4SFP-B, IOC-S-2SFP+, IOC-S-2SFP+B, IOC-S-4SFP+, IOC-S-4SFP+B | IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-4SFP-B, IOC-S-2SFP+, IOC-S-2SFP+B, IOC-S-4SFP+, IOC-S-4SFP+B | IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-4SFP-B, IOC-S-2SFP+, IOC-S-2SFP+B, IOC-S-4SFP+, IOC-S-4SFP+B | IOC-S-4GE-B-H, IOC-S-4SFP-H, IOC-S-8GE-B-H, IOC-S-8SFP-H, IOC-S-4SFP-B-H, IOC-S-2SFP+H, IOC-S-4SFP+H, IOC-S-2SFP+B-H, IOC-S-4GE-4SFP-H |
| <b>Latency</b>  | <100 µs                             | <100 µs                             | <100 µs                             | <100 µs  | <100 µs  | <100 µs  | <100 µs  | <100 µs  |
| <b>Bypass Support (Default/Max.)</b>  | 4/8                                 | 4/8                                 | 4/8                                 | 4/20   | 4/20   | 6/22   | 6/22   | 0/32   |
| <b>Power Supply</b>   | 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  | AC 100-240 V 50/60 Hz  | AC 100-240 V 50/60 Hz  | AC 100-240 V 50/60 Hz  |
| <b>Maximum Power Consumption</b>  | 1 x 60W                             | 1 x 60W                             | 1 x 60W                             | 250W Redundancy 1 + 1  | 250W Redundancy 1 + 1  | 350W Redundancy 1 + 1  | 350W Redundancy 1 + 1  | 350W Redundancy 1 + 1  |
| <b>Dimension (WxDxH, mm)</b>  | 16.9 x 11.8 x 1.7 in (430x300x44mm) | 16.9 x 11.8 x 1.7 in (430x300x44mm) | 16.9 x 11.8 x 1.7 in (430x300x44mm) | 16.9 x 14.8 x 1.7 in (430x375x44mm)  | 16.9 x 14.8 x 1.7 in (430x375x44mm)  | 16.9 x 19.7 x 3.5 in (430x500x88mm)  | 16.9 x 19.7 x 3.5 in (430x500x88mm)  | 16.9 x 19.7 x 3.5 in (430x500x88mm)  |
| <b>Weight</b>   | 14.3 lb (6.5 kg)                    | 14.3 lb (6.5 kg)                    | 14.3 lb (6.5 kg)                    | 22.0 lb (10 kg)  | 22.0 lb (10 kg)  | 35.3 lb (16 kg)  | 35.3 lb (16 kg)  | 35.3 lb (16 kg)  |
| <b>Temperature</b>  | 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)  | 32-104°F (0-40°C)  | 32-104°F (0-40°C)  |
| <b>Relative Humidity</b>  | 5-85% (no dew)                      | 5-85% (no dew)                      | 5-85% (no dew)                      | 5-85% (no dew)   | 5-85% (no dew)   | 5-85% (no dew)   | 5-85% (no dew)   | 5-85% (no dew)   |

## Opções de Módulo

| Module    | IOC-S-4GE-B-L                 | IOC-S-4SFP-L                  | IOC-S-4GE-B                   | IOC-S-4SFP                    | IOC-S-8GE-B                   | IOC-S-8SFP                    | IOC-S-4GE-4SFP                |
|-----------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|
| I/O Ports | 4 x GE Bypass Ports           | 4 x SFP Ports                 | 4 x GE Bypass Ports           | 4 x SFP Ports                 | 8 x GE Bypass Ports           | 8 x SFP Ports                 | 4 x GE and 4 x SFP Ports      |
| Dimension | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) |
| Weight    | 0.22 lb (0.1 kg)              | 0.22 lb (0.1 kg)              | 0.33 lb (0.15 kg)             | 0.33 lb (0.15 kg)             | 0.55 lb (0.25 kg)             | 0.55 lb (0.25 kg)             | 0.55 lb (0.25 kg)             |

| Module    | IOC-S-2SFP+                   | IOC-S-4SFP+                   | IOC-S-4SFP-B                  | IOC-S-2SFP+-B                 | IOC-S-4SFP+-B                 | IOC-S-4GE-B-H                 | IOC-S-4GE-4SFP-H              |
|-----------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|
| I/O Ports | 2 x SFP+ Ports                | 4 x SFP+ Ports                | 4 x SFP Bypass Ports          | 2 x SFP+ Bypass Ports         | 4 x SFP+ Bypass Ports         | 4 x GE Bypass Ports           | 4 x GE and 4 x SFP Ports      |
| Dimension | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) |
| Weight    | 0.33 lb (0.15 kg)             | 0.44 lb (0.2 kg)              | 0.88 lb (0.4 kg)              | 0.88 lb (0.4 kg)              | 0.88 lb (0.4 kg)              | 0.33 lb (0.15 kg)             | 0.55 lb (0.25 kg)             |

| Module    | IOC-S-8GE-B-H                 | IOC-S-8SFP-H                  | IOC-S-4SFP-H                  | IOC-S-2SFP+-H                 | IOC-S-4SFP+-H                 | IOC-S-4SFP-B-H                | IOC-S-2SFP+-B-H               |
|-----------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|
| I/O Ports | 8 x GE Bypass Ports           | 8 x SFP Ports                 | 4 x SFP Ports                 | 2 x SFP+ Ports                | 4 x SFP+ Ports                | 4 x SFP Bypass Ports          | 2 x SFP+ Bypass Ports         |
| Dimension | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) | 1 U (Occupies 1 generic slot) |
| Weight    | 0.55 lb (0.25 kg)             | 0.55 lb (0.25 kg)             | 0.33 lb (0.15 kg)             | 0.33 lb (0.15 kg)             | 0.44 lb (0.2 kg)              | 0.88 lb (0.4 kg)              | 0.88 lb (0.4 kg)              |

### OBSERVAÇÕES:

- (1) IPS Throughput data is obtained under HTTP traffic with all IPS rules being turned on;
- (2) Maximum Concurrent Connections are obtained under TCP traffic; and it can be upgraded with Additional Enhanced License (AEL);
- (3) New Sessions are obtained under TCP traffic.

A menos que especificado de outra forma, todos os recursos, funções e o desempenho são baseados no StoneOS5.5R5. Os resultados podem variar dependendo da versão e implementação do StoneOS®.