Hillstone CloudEdge:
Virtual Next-Generation Firewall

O Hillstone Virtual Next-Generation Firewall, CloudEdge, com o sistema operacional Hillstone Networks StoneOS, é implementado como uma máquina virtual e oferece serviços avançados de segurança para aplicações e usuários em qualquer ambiente virtualizado. Ele fornece abrangentes recursos de segurança, incluindo identificação e controle granular de aplicação, VPN, prevenção de intrusão, antivírus, contra-ataque e sandbox de nuvem para manter seu negócio totalmente seguro e operacional. Ele oferece soluções de preço-desempenho para clientes de nuvem pública e nuvem privada, e pode ser rapidamente provisionado e implementado em escala.

Destaques do Produto

Altamente Compatível com Ambientes Virtuais

Em ambientes virtuais, os recursos de computação, armazenamento e de dados são executados em máquinas virtuais. O Hillstone CloudEdge suporta a maioria das tecnologias hypervisor, incluindo ESXi, KVM, Hyper-V e servidor Xen, e pode ser rapidamente implementado em uma máquina virtual para fornecer serviços avançados de segurança para redes virtuais ou aplicações virtualizadas. Implementado como um dispositivo virtual, o CloudEdge pode sobrepujar a limitação de firewalls físicos e inspecionar todo o tráfego tanto sul-norte quanto leste-oeste. Além disso, os usuários têm flexibilidade para implementar e gerenciar recursos de rede com base nos requisitos de topologia de rede e, assim, aproveitar todas as vantagens da vitalização.

Recurso Avançado de Proteção contra Ameaças

O CloudEdge compartilha uma tecnologia base com o Hillstone Next-Generation Firewall (NGFW). Ele pode atender aos requisitos de segurança de rede para usuários de nuvem pública e nuvem privada. O Hillstone CloudEdge oferece controle granular de aplicações da Web independentemente de porta, protocolo ou ação evasiva. Ele pode identificar e evitar possíveis ameaças associadas a aplicações de alto risco e, ao mesmo tempo, fornecer controle baseado em políticas para aplicações, usuários e grupos de usuários. Além disso, o CloudEdge incorpora um mecanismo unificado de detecção de ameaças que compartilha detalhes de pacote com vários mecanismos de segurança (AD, IPS, filtro de URL, Antivírus, Sandbox de nuvem etc.), o que aumenta significativamente a eficiência de segurança e reduz a latência da rede.

Destaques do Produto (Continuação)

Gerenciamento Visualizado de Segurança com Plataforma de Gerenciamento de Nuvem

O Hillstone CloudEdge oferece exclusiva segmentação de segurança e proteção de política para usuários independentes em implementações na nuvem. Ele pode realizar recuperação instantânea baseada no sistema de instantâneo. Se um dispositivo virtual tiver um problema ou uma parada, ele poderá ser recuperado a partir do instantâneo de uma configuração salva, e começar um novo firewall virtual na máquina original ou em uma nova máquina virtual. A interface gráfica de gerenciamento do CloudEdge possui diversas funções de consulta de logs, o que pode efetivamente monitorar e acompanhar o status da rede, e uma função de relatórios que oferece detalhes em tempo real de tráfego e eventos de segurança. Essas ferramentas ajudam administradores a visualizar e compreender completamente o status de operação da rede e aprimorar a eficiência operacional.

Automação de Implementação e Orquestração de Serviços

O Hillstone CloudEdge oferece várias soluções integradas para satisfazer necessidades e requisitos de plataformas de nuvem e já foi implementado em diversos ambientes de nuvem de teste e de produção para atender a várias indústrias e requisitos do cliente. As funções de implementação de automação e gerenciamento de licenças oferecem ao usuário de nuvem a habilidade de autosserviço e autogerenciamento baseada em suas necessidades de negócio sem interrupção de administradores de nuvem. A orquestração garante que cada CloudEdge possa ser implementado e configurado automaticamente. O gerenciamento de licenças garante que o CloudEdge possa entrar automaticamente no modo de operação. A API REST do Hillstone CloudEdge suporta configuração de sistema, configuração de política de segurança, configurações de interfaces e rede, para integração com as principais plataformas de gerenciamento de nuvem.

Recursos

Serviços de Rede
- Roteamento dinâmico (OSPF, BGP, RIPv2)
- Roteamento Estático e de Política
- Roteamento controlado por aplicação
- Servidor DHCP, NTP, DNS e proxy DNS incorporado
- Modo tap - Conecta-se com a porta SPAN
- Modos de interface: sniffer, porta agregada, loopback, VLANS (802.1Q e Trunking)
- Comutação e roteamento L2/L3
- Implementação virtual em linha transparente de wire (Camada 1)

Firewall
- Modos de operação: NAT/rota, transparente (ponte) e modo combinado
- Objetos de política: predefinido, personalizado e agrupamento de objetos
- Política de segurança com base na aplicação, função e geolocalização
- Gateways no nível da aplicação e suporte a 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 de NAT: por política e tabela NAT central
- VoIP: SIP/H.323/SCCP NAT traversal, RTP pin holing
- Visualização de gerenciamento de política global
- Inspeção de redundância de política de segurança, política grupo, politica de configuração rollback
- Política abrangente de DNS
- Programações: única e recorrente
- Asistente para una implementación fácil y detallada de políticas
- Análisis y limpieza de políticas inválidas

Prevenção de Intrusão
- Detecção de anomalia de protocolo, detecção baseada em taxa, assinaturas personalizadas, push manual, automático ou atualizações de assinatura de pull, enciclopédia integrada de ameaças
- Ações IPS: padrão, monitorar, bloquear, redefinir (IP do atacante ou da vítima, interface de entrada) com tempo de expiração
- Opção de registro de pacote
- Seleção Baseada em Filtro: gravidade, alvo, 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, TCP/UDP/SCTP port scan, ICMP sweep, flood de sessão TCP/UDP/SCIP/ICMP (fonte/destino)
- Bypass ativo com interfaces de bypass
- Configuração de prevenção predefinida

Antivírus
- Push manual, automático ou atualizações de assinatura de pull
- Antivírus baseado em fluxo: os protocolos incluem HTTP, SMTP, POP3, IMAP, FTP/SFTP
- Varredura de vírus em arquivo compactado

Defesa de Ataque
- Defesa de ataque de protocolo anormal
- Defesa contra DoS/DDoS, incluindo Flood de SYN, flood de DNS Query
- Defesa de ataque ARP

Filtro de URL
- Inspeção de filtro de Web baseada em fluxo
- Filtro de Web definido manualmente com base em URL, conteúdo da Web e cabeçalho MIME
- Filtro dinâmico da Web com banco de dados de categorização em tempo real baseado na nuvem: mais de 140 milhões de URLs com 64 categorias (8 dos quais são relacionados a segurança)
- Recursos adicionais de filtro de Web:
  - Filtrar Java Applet, ActiveX ou cookie
  - Bloquear post HTTP
  - Registrar palavras-chave de busca
  - Isentar conexões criptografadas de varredura em determinadas categorias de 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 classificação de categoria de filtro de Web

Sandbox de Nuvem
- Carregamento de arquivos maliciosos em sandbox de nuvem para análise
- Protocolos de suporte, incluindo HTTP/HTTPS, POP3, IMAP, SMTP e FTP
- Tipos de arquivo de suporte, incluindo PE, ZIP, RAR, Office, PDF, APK, JAR e SWF
- 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

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
- IP e domínio de lista de permissões

Recursos (Continuação)

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

Identificação de Endpoint
- Suporte para identificar IP de endpoint, quantidade de endpoints, tempo online, tempo offline e duração online
- Soporta 10 sistemas operativos incluyendo 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
- Después de bloquear al usuario, puedes redireccionar al usuario a una página específica
- Soporta bloqueo de operaciones en desbordamiento de IP

Segurança de Dados
- Controle de transferência de arquivo baseado no tipo de arquivo
- Identificação de protocolo de arquivo, incluindo HTTP, FTP, SMTP e POP3
- Assinatura de arquivo e identificação de sufixo para mais de 100 tipos de arquivo
- Filtro de conteúdo para protocolos HTTP-GET, HTTP-POST, FTP e SMTP
- Identificação IM e auditoria de comportamento de rede

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
- Limpieza automática y manual del tráfico expirado utilizado por el usuario

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
- O balanceamento de carga de link de saída inclui roteamento baseado em política, ECMP e ponderação, roteamento ISP incorporado e detecção dinâmica
- 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, aplicativo 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 Fase1/Fase2: DES, 3DES, AES128, AES192, AES256
  - Autenticação de proposta Fase1/Fase 2: MD5, SHA1, SHA256, SHA384, SHA512
  - Suporte a Diffie-Hellman Fase 1/Fase 2: 1,2,5
  - 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 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

Alta Disponibilidade
- Interfaces heartbeat redundantes
- Ativo/Passivo
- Sincronização de sessão autônoma
- Interface de gerenciamento reservada para HA
- Failover:
  - Monitoramento de porta, local e link remoto
  - Failover stateful
  - Failover sub-secundário
  - Notificação de falha
- Opções de implementação:
  - HA com agregação de link
  - HA full mash
  - HA geograficamente disperso

Decodificação de SSL
- Identificação de aplicativo para tráfego criptografado por SSL
- Ativação IPS para tráfego criptografado SSL
- Habilitação AV para tráfego criptografado SSL
- Filtro de URL para tráfego criptografado por SSL
- Lista de permissões de tráfego SSL criptografado
- Modo de descarregamento do proxy SSL

Identidade de Usuário e Dispositivo
- Banco de dados local de usuários
- Autenticação remota de usuário: TACACS+, LDAP, Radius, Active
- Login único: Windows AD
- Autenticação de dois fatores: suporte a terceiros, servidor de token integrado com físico e SMS
- Políticas de usuário e baseadas em dispositivo
- Sincronização de grupo de usuários baseada em AD e LDAP
- Suporte a 802.1X, proxy SSO
- Personalização de página WebAuth
- Autenticação baseada em interface
- ADSSO sem agente (AD Polling)
- Sincronização de autenticação de uso baseada em monitor SSO
- Suporte a autenticação de usuários MAC-based

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 alianças
- Implementação rápida: instalação automática 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
- Recursos de log: memória e armazenamento local (se disponível), diversos servidores syslog e diversas plataformas Hillstone Security Audit (HSA)
- Log criptografado e integridade de log com carregamento de log HSA em lote programado
- Log confiável usando opção TCP (RFC 3195)
- Logs detalhados de tráfego: encaminhado, sessões violadas, tráfego local, pacotes inválidos, URL etc.
- Logs abrangentes de eventos: auditorias de sistema e atividade administrativa, roteamento e rede, VPN, autenticação de usuário, eventos relacionados a Wi-Fi
- Opção de resolução de IP e nome de porta de serviço
- Opção de formato abreviado de log de tráfego
- Três relatórios predefinidos: relatórios de segurança, fluxo e rede
- Relatórios definidos pelo usuário
- Os relatórios podem ser exportados em PDF por email e FTP

Recursos (Continuação)

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)

Gerenciamento de Licenças

- Ativação/desativação automática de licença
- Usuários de nuvem pública ou nuvem privada com acesso à internet
- Movimentação de licença com dispositivo

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

REST API

- Login, monitoramento de dispositivo
- Catálogo de endereços, serviços e aplicações
- Política de aplicação, política AV, política IPS, DNAT/SNAT, política de segurança
- Configuração: Configuração de interface, configuração de roteamento, configuração de zona

Virtualização

- Hypervisor: KVM, VMware ESXi, Xen, AMI (AWS), Hyper-V
- Nuvem Pública: AWS, Azure, AliCloud etc.
- Plataforma de Gerenciamento de Nuvem: Openstack Liberty e versões superiores, VMware vCenter 5.5 e versões superiores etc.
- Plataforma Array AVX Series Network Functions

Especificações do Produto

	VM01	VM02	VM04
Core (Min)	2	2	4
Memory (Min)	2 GB	4 GB	8 GB
Storage (Min)	4 GB	4 GB	4 GB
Network Interfaces	10	10	10
Firewall Throughput (vNIC/SR-IOV)	2 Gbps / 10 Gbps	4 Gbps / 20 Gbps	8 Gbps / 30 Gbps
IPS Throughput (vNIC/SR-IOV)	1 Gbps / 3 Gbps	2 Gbps / 5 Gbps	4 Gbps / 7 Gbps
AV Throughput (vNIC/SR-IOV)	800 Mbps / 1 Gbps	1.6 Gbps / 2 Gbps	3.2 Gbps / 4 Gbps
IMIX Throughput (vNIC/SR-IOV)	550 Mbps / 1.6 Gbps	1.3 Gbps / 2.1 Gbps	1.3 Gbps / 2.6 Gbps
NGFW Throughput (vNIC/SR-IOV)	700 Mbps / 1.5 Gbps	1.4 Gbps / 2.5 Gbps	2.8 Gbps / 3.5 Gbps
Threat Protection Throughput (vNIC/SR-IOV)	400 Mbps / 500 Mbps	800 Mbps / 1 Gbps	1.6 Gbps / 2 Gbps
IPsec VPN Throughput (vNIC/SR-IOV)	200 Mbps / 400 Mbps	400 Mbps / 800 Mbps	800 Mbps / 2 Gbps
New Sessions / Second(vNIC/SR-IOV)	20,000 / 30,000	40,000 / 50,000	80,000 / 100,000
Maximum Concurrent Sessions	100,000	500,000	5 Million
IPSec VPN Tunnels (Max.)	100	500	10,000
SSL VPN Users (Max.)	100	500	2,000

OBSERVAÇÃO:

O desempenho acima foi observado usando um servidor Dell R720 (Intel (R) Xeon (R) CPU E5-2680 v2 @ 2.70GHz, 64GB de memória, 4x 10 interfaces GE), VMXnet3 em ambiente VMware. O SR-IOV foi observado no KVM.

A menos que especificado de outra forma, todos os recursos, funções e o desempenho são baseados no StoneOS5.5R7. Os resultados podem variar dependendo da versão e implementação do StoneOS®.

Versão: EX-08.01-CloudEdge-5.5R7-1020-PT-01