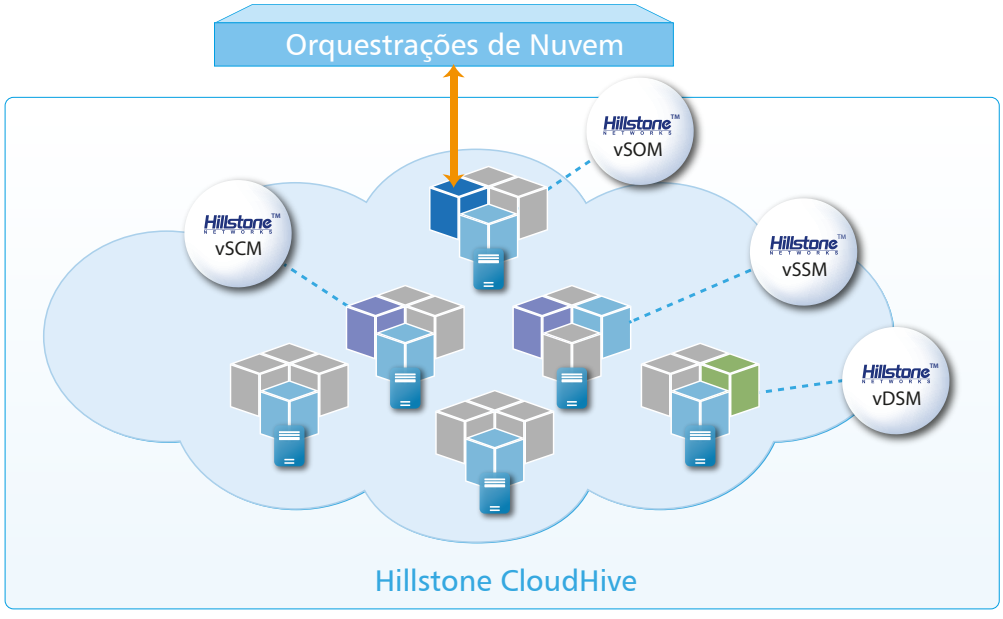
Hillstone CloudHive:
Solução de Microssegmentação para a Nuvem

O Hillstone CloudHive oferece tecnologia de microssegmentação para garantir cada implementação de máquina virtual (VM) na nuvem. Ele oferece abrangente visibilidade de tráfego Leste-Oeste e fornece proteção completa para parar ataques laterais entre as VMs. Além disso, o serviço de segurança CloudHive pode ser facilmente escalado para satisfazer necessidades de negócio sem interrupção.

O Hillstone CloudHive é formado por quatro tipos de módulos virtuais que trabalham juntos como um único dispositivo para fornecer segurança completa para cada VM.

- O Módulo Virtual de Orquestração de Segurança (vSOM), integrado e conectado com as Plataformas de Gerenciamento de Nuvem (CPMs), gerencia o ciclo de vida do serviço CloudHive.
- O Módulo Virtual de Controle de Segurança (vSCM) é o painel de controle, que suporta configuração e distribuição de política, bem como gerencia o ciclo de vida do vSSM.
- O Módulo Virtual de Serviço de Segurança (vSSM) é implementado em cada servidor físico para implementar microssegmentação e fornecer serviços de segurança L2-L7.
- O Módulo Virtual de Serviço de Dados (vDSM) é um módulo de encaminhamento de log opcional que envia logs do CloudHive para servidores syslog externos. Ele suporta o envio em massa de logs pela implementação de balanceamento de carga de vários módulos.



Destaques do Produto

Obtém Visibilidade Inigualável de Tráfego ao Vivo

Todos os pontos de acesso às máquinas virtuais podem ser monitorados para fornecer visibilidade de tráfego, aplicações e ameaças relacionadas à VM ou ao grupo de portas, o que é fundamental para permitir controle e proteção de tráfego Leste-Oeste. Um novo tráfego e uma nova aplicação durante um período específico podem ser monitorados e visualizados para exibir as mudanças sutis na rede virtual. Topologia de VM, insights sobre o tráfego, identificação da aplicação, bem como abrangentes recursos de log permitem que Provedores de Serviço na Nuvem (CSPs) satisfaçam requisitos de conformidade e auditoria de segurança.

Reduz a Superfície de Ataque a Praticamente Zero

Cada Módulo de Serviço de Segurança Virtual (vSSM) CloudHive é implementado em um servidor físico, permitindo a microssegmentação para comunicação inter-VM ou inter-rede. O tráfego Leste-Oeste é protegido com serviços de segurança L2-L7, incluindo recursos de firewall como controle de política e limites de sessão, recursos avançados de segurança como Sistema de Prevenção de Intrusão (IPS), Antivírus e Contra-Ataque (AD), bem como controle fino da aplicação. A mitigação em tempo real também bloqueia, impede ou coloca em quarentena ataques ativos.

Dimensiona Sem Esforço a Segurança pela Orquestração Ativa

O CloudHive integra-se perfeitamente às principais plataformas de virtualização, incluindo VMware e Openstack, e tem o VMware Ready certificado com a integração NSX.Serviços de segurança sob demanda podem ser aplicados a todas as cargas de trabalho e às VMs pela escalabilidade do vS SM. A implementação do vSCM permite configuração unificada de política de segurança para cada VM. O CloudHive suporta vMotion para garantir que os serviços de segurança persistam em caso de movimentação da VM. Os fluxos de VM existentes não serão interrompidos pelo vMotion.

Melhora a Eficiência e Reduz Custos

A implementação do CloudHive Camada 2 não afeta a topologia existente da rede. Junto com ferramentas e recursos únicos de otimização de configuração, ele minimiza os custos gerais de implementação e configuração sem impacto nos negócios ou interrupção da rede. Além disso, a vantagem da facilidade de gerenciamento de um único dispositivo reduz erros operacionais e melhora a eficiência geral. O custo total de propriedade também é reduzido, uma vez que os serviços de segurança do CloudHive não exigem nenhuma atualização ou expansão das atuais plataformas de nuvem.

Monitoramento em Tempo Real do Desempenho do Serviço

O CloudHive mergulha profundamente no ambiente de nuvem para criar a primeira linha de segurança e defesa para máquinas virtuais e para os dados e aplicativos críticos que residem nelas.
Como as inter-relações entre vários sistemas e serviços de negócios no ambiente em nuvem são complexas, o CloudHive fornece gerenciamento de desempenho de rede do ponto de vista comercial.
O CloudHive descobre e define automaticamente dependências de serviço dentro e fora do datacenter e estabelece um relacionamento de referência entre os serviços de um determinado negócio.
Em seguida, monitora o atraso e a tremulação de cada serviço, o atraso, a tremulação e a perda de pacotes de cada rede e a utilização da CPU e da memória da máquina virtual. Assim, o CloudHive fornece monitoramento completo das cadeias de serviços em termos de qualidade de serviço, qualidade da rede e recursos de computação, além de fornecer recursos de solução rápida de problemas com análise avançada de dados.

Recursos

Controle de Aplicação
- Mais de 4,000 aplicações que podem ser filtradas por nome, categoria, subcategoria, tecnologia e risco
- Cada aplicação contém uma descrição, fatores de risco, dependências, portas típicas utilizadas e URLs para referência adicional
- Ações: bloquear, redefinir sessão, monitorar, shaping de tráfego
- Atualização do banco de dados de aplicações em tempo real

Visibilidade
- Descoberta automáticade ativo virtual: redes e VMs
- Monitor dinâmico de ativo virtual, atualização automática/manual de agenda de endereços VM/IP/MAC
- Gerenciamento virtual de grupo de ativos, sincronização automática / manual das informações de agrupamento de ativos
- Visualização de topologia de rede virtual, VMs e tráfego
- Insight profundo e monitoramento de todo o tráfego entre VMs ou grupos de portas
- Classificação de tráfego, aplicação e ameaça, detalhamento de informações relacionadas.
- Opções de Visualização Personalizada: classificar, consultar, filtrar, ampliar/reduzir.
- Suporte a log: logs de sessão, logs de ameaça e logs de sistema

Serviço de Monitoramento de Desempenho
- Monitoramento multidimensional da qualidade do desempenho do serviço em nuvem, incluindo utilização de recursos, qualidade da rede e serviços
- Consulta de dados de monitoramento com monitoramento flexível por ponto e intervalo
- Topologia automática da cadeia de serviços, apresentando as comunicações internas e externas dos serviços em nuvem
- Transmissão de tela para uma visão global

Firewall
- Controle de acesso Camada 2-Camada 7
- Controle de acesso com base em VM e grupo de portas
- Controle de acesso com base na conta do AD
- Controle de acesso com base na tabela de horário
- Gateway da Camada da Aplicação (ALG)
- Limite de sessão: Nova Sessão/Sessão Simultânea

Contra-Ataque
- Contra-ataque de protocolo anormal
- Anti-DoS/DDoS, incluindo defesa SYN Flood, DNS Query Flood
- Contra-ataque ARP
- Detecção e defesa de varredura de porta

Prevenção de Intrusão
- Ações de IPS: padrão, monitorar, bloquear, redefinir (IP do atacante ou IP da vítima, interface de entrada) com tempo de expiração
- Detecção de anomalia de protocolo, detecção baseada em taxa, assinaturas personalizadas, atualizações de assinatura por push ou pull manuais e automáticas, enciclopédia de ameaça integrada
- Opção de log de pacote
- Seleção Baseada em Filtro: gravidade, alvo, SO, aplicação ou protocolo
- Isenção de IP de assinaturas IPS específicas
- Modo sniffer IDS
- Proteção 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

Antivírus
- Atualizações de assinatura por push ou pull manuais e automáticas
- Antivírus com base no fluxo: os protocolos incluem HTTP, SMTP, POP3, IMAP, FTP/SFTP
- Varredura de vírus em arquivo compactado

Filtragem de URL
- Controle de acesso a páginas da Web com base em IP, VM, atributos de grupo de serviços
- Suporte a mais de 60 categorias, dezenas de milhões de assinaturas de URL, categorias de URL personalizáveis
- Atualização em tempo real do banco de dados de assinatura de URL

Implementação
- Suporta modo tapping e modo em linha transparente
- Implementação L2 sem a necessidade de alterações na configuração da rede
- Facilidade de implementação sem autoridade raiz e qualquer plug-in, efeito minimizado à VM e ao hypervisor.
- vSSM pode escalar até 200 módulos vSSM sem interrupção do serviço de segurança
- Obtém configuração de política com base na VM por aprendizado automático em ativos virtuais.
- Detecta o estado da VM (acima ou abaixo), e atualiza alteração de IP da VM automaticamente
- Habilita ou desabilita com um clique o serviço de segurança na VM ou grupo de portas
- Suporta implementação de VMware VSS/VDS, vSAN
- Suporta implementação de Openstack OVS

Alta Disponibilidade
- A "Finalização de VM" do vSOM não afeta o serviço CloudHive
- vSOM pode ser implementado em pares (Ativo/Passivo) para prover alta disponibilidade
- Separação de gerenciamento, controle e plano de serviço garante a estabilidade do serviço
- O vSCM é implementado em pares (Ativo/Passivo) para fornecer alta disponibilidade
- A "Finalização de VM" de vSSM único não afeta o sistema; o tráfego da VM do usuário pode contornar o vSSM
- O vSCM pode ser reiniciado e reinicializar automaticamente o serviço de segurança após a "finalização de VM".
- Suporte a vMotion: a política de segurança e as sessões de fluxo são automaticamente sincronizadas nos vários módulos de serviço
- Suporte para Atualização de Software de Serviço (ISSU)
- Suporta controle de host de administração de rede confiável e controle de tentativas de login

Gerenciamento
- Interface: API RESTful, CLI, WebUI
- Arquitetura distribuída, gerenciamento centralizado e unificado por meio de uma interface única
- Envio de log a servidores syslog externos pelo vDSM, suporta o envio em massa de log em alta velocidade.
- Suporta Radius/TACACS+ de terceiros
- Suporta controle com base em IP/Porta/App e em grupo de VM/Porta
- Suporte a políticas de auto-aprendizagem / agrupamento / convergência, remoção de itens duplicados e contagem de ocorrências
- Suporte total a IPv6, suporta atualização de IPv4 para IPv6
- RestAPI para desenvolvimento adicional de automação e integração
- Monitoramento de SNMP e alarme de trap SNMP, suporte a NTP.
- Modo de administração multicamada para a separação de operação e gerenciamento.
- Captura e download de pacote, diagnóstico de alteração de ambiente para localização de falha
- Importar/Exportar políticas e configurações

Recurso de Virtualização
- VMware vSphere 5.0/5.1/5.5/6.0/6.5/7.0
- VMware NSX 6.2/6.3/6.4
- VMware Horizon VDI platform
- FusionSphere OpenStack 6.1/6.3/6.5
- FusionCompute 6.5.1, 8.0.0, 8.0.1

Especificações do Produto

Module	Description	System Resource	Module #
vSOM	Módulo de Orquestração de Segurança Virtual	2*vCPU, 2GB Memory, 12GB Hard Disk	1 Standard
vSCM	Virtual Security Control Module	2*vCPU, 6GB Memory, 17GB Hard Disk	1 Min., 2 Recommended
vSSM (Padrão)	Virtual Security Service Module 02	2*vCPU, 4GB Memory, 5GB Hard Disk	200 máx.
vSSM (Avançado)	Virtual Security Service Module 04	4*vCPU, 8GB Memory, 5GB Hard Disk	Quando implantado no modo Jumbo Frame, o requisito de memória será aumentado em 2G na base original.
vDSM	Módulo de Serviço de Dados Virtuais	2*vCPU, 4GB Memory, 5GB Hard Disk	Optional, multiple mode supported

Sistema CloudHive	vSSM 02	vSSM 04
Firewall Throughput (Maximum)	1 Tbps	1 Tbps
Maximum Concurrent Sessions	340 Million	680 Million
New Sessions/s (HTTP)	6 Million	10 Million
IPS Throughput (Maximum)	300 Gbps	1 Tbps
AV Throughput (Maximum)	300 Gbps	1 Tbps
vSSM Scalability (Maximum)	200	200

VSSM Individual	vSSM 02	vSSM 04
Firewall Throughput [1]	5 Gbps	5 Gbps
Firewall Throughput (NSX) [2]	16 Gbps	16 Gbps
Maximum Concurrent Sessions	1.7 Million	3.4 Million
New Sessions/S (HTTP)	30,000	50,000
IPS Throughput [3]	1.5 Gbps	5 Gbps
AV Throughput [4]	1.5 Gbps	5 Gbps

NOTES:

(1) Todos os dados de desempenho são obtidos no ambiente DellR720, VMware, VDS;

(2) Todos os dados de desempenho são obtidos no ambiente DellR720, VMware(6.0U2), VDS, NSX(v6.4);

(3) os dados de capacidade IPS são obtidos com detecção de tráfego HTTP bidirecional com todas as regras de IPS desativadas;

(4) os dados de capacidade AV são obtidos em tráfego HTTP com anexação de arquivo de 512 KB.

Salvo indicação em contrário, todo desempenho, capacidade e funcionalidade são baseados no StoneOS 5.5R3. Os resultados reais podem variar devido às versões do software CloudHive e ao ambiente de implantação.

Versão: EX-08.01-CloudHive-V2.7.3.1-0321-PT-01