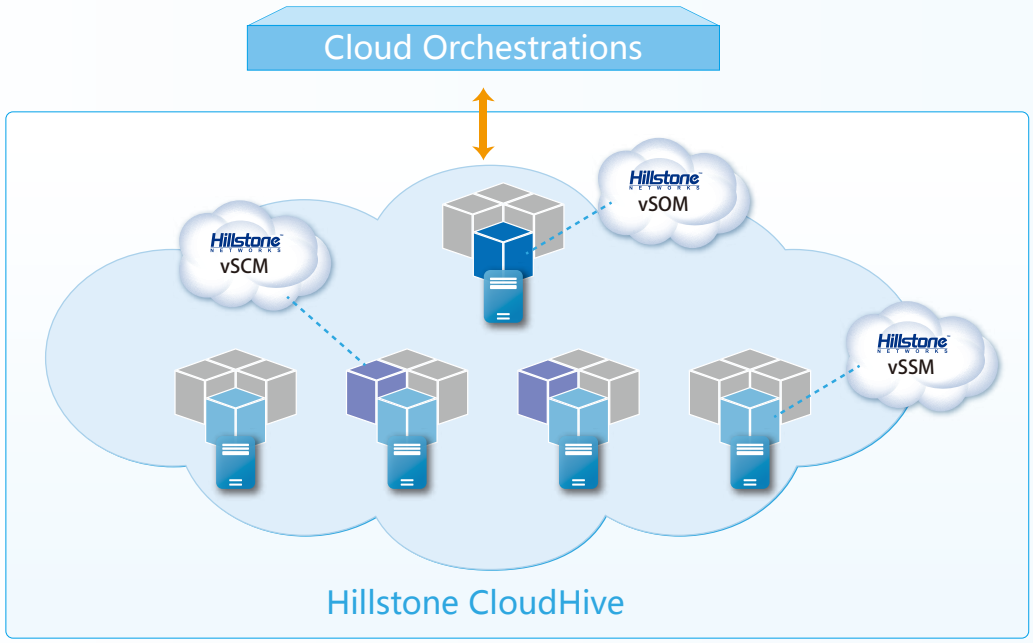
Hillstone CloudHive:

Micro-segmentation Solution for the Cloud

Hillstone CloudHive provides micro-segmentation to secure each virtual machine (VM) in the cloud. It provides comprehensive visibility of East-West traffic and provides complete protection to stop lateral attacks between VMs. In addition, the CloudHive security service can scale easily to meet demand without business interruption.

Hillstone CloudHive is comprised of three types of virtual modules that work together as a single appliance to provide complete security to each virtual machine. The Virtual Security Orchestration Module (vSOM), integrated and connected with Cloud Management Platforms (CMPs), manages the CloudHive service lifecycle. The Virtual Security Service Module (vSSM) is deployed on each physical server to provide L2-L7 security services. The Virtual Security Control Module (vSCM) is the control panel, supporting policy configuration and distribution, as well as managing the lifecycle of the vSSM.



www.hillstonenet.com
Phone: 1-800-889-9860

Product Highlights

- **Achieve Unparalleled Live Traffic Visibility :**
  All virtual machine access points can be monitored to provide visibility and control of traffic, applications and attacks inter-VM; which is the cornerstone for enabling East-West traffic control and protection. VM topology, traffic insight, application identification, as well as comprehensive log features allow Cloud Service Providers (CSPs) to meet compliance and security audit requirements.

- **Reduce Attack Surface to Nearly Zero:**
  Each CloudHive Virtual Security Service Module (vSSM) is deployed on a physical server, enabling micro-segmentation for inter-VM communication. East-West traffic is secured with L2-L7 security services, including firewall features such as policy control and session limits, advanced security features such as Intrusion Prevention System (IPS) and Attack Defense (AD), as well as fine-grained application control. Real-time mitigation also blocks, impedes or quarantines active attacks.

- **Effortlessly Scale Security Through Active Orchestration:**
  On-demand security services can be applied to any and all new workloads and VMs through the scalability of vSSM. The deployment of vSOM enables unified security policy configuration for each VM. CloudHive supports vMotion to ensure security services persist in the event the VM moves.

- **Improve Efficiency While Reducing Costs:**
  CloudHive Layer 2 deployment does not impact existing network topology. It minimizes deployment and configuration overhead, without business impact or network interruption. In addition, the ease of management advantage of a single appliance reduces operational errors and improves overall efficiency. Total cost of ownership is also reduced as CloudHive security services do not need to upgrade to VMware's NSX.

Product Features

Application Control
- Over 3,000 applications that can be filtered by name, category, subcategory, technology and risk
- Each application contains a description, risk factors, dependencies, typical ports used, and URLs for additional reference
- Actions: block, reset session, monitor, traffic shaping

Visibility
- Cloud asset discovery: networks and VMs
- Visualization of virtual network topology, VMs and traffic
- Deep insight and monitoring of all traffic between VMs
- Log support: session logs, threat logs and system logs

Firewall
- Policy control
- Application Layer Gateway (ALG)
- Session limit

IPS
- 7,000+ signatures, including custom signatures
- Protocol anomaly detection
- Manual, automatic signature updates
- Integrated threat encyclopedia
- IPS Actions: default, monitor, block, reset with expiry time
- Packet logging option
- Filter Based Selection: severity, target, OS, application or protocol
- IP exemption from specific IPS signatures
- IDS sniffer mode

Attack Defense
- Protection from: Malformed packets, DoS/DDoS, DNS Query Flood, SYNFlood and ARP attacks

High Availability
- Separation of management, control and service plane
- vSOM "VM shutdown" does not affect the CloudHive service
- vSCM are deployed in pairs (Active/Passive) to provide high availability
- vSSM "VM down" does not affect the workload as it is deployed on a separate VM

Scalability
- vSSM can scale up to 200 modules

Deployment
- Supports both tapping mode and inline mode
- L2 deployment without the need for network configuration changes

Cloud Management Platform
- VMware vCenter 5.5
- Interface: RESTful API, CLI, WebUI
- vMotion support
- Dynamic address book

Hypervisor Compatibility
- VMware ESXi

Specifications

Each of the three types of virtual modules that comprise CloudHive requires a VM with 2 CPU cores and 4GB memory.

Specification	CloudHive System
Firewall Throughput (Maximum)	1 Tbps
Maximum Concurrent Sessions	340 Million
New Sessions/s	6 Million
IPS Throughput (Maximum)	200 Gbps
vSSM Scalability (Maximum)	200

Specification	Each vSSM
Firewall Throughput	5 Gbps
Maximum Concurrent Sessions	1.7 Million
New Sessions/s	30,000
IPS Throughput	1 Gbps

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS 5.5R1. Results may vary based on StoneOS® version and deployment.