Hillstone CloudHive: Micro-segmentation Solution for the Cloud

Hillstone CloudHive provides micro-segmentation technology to secure each virtual machine (VM) in cloud deployments. 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.

- Virtual Security Orchestration Module (vSOM), integrated and connected with Cloud Management Platforms (CMPs), manages the CloudHive service lifecycle.
- Virtual Security Service Module (vSSM) is deployed on each physical server to implement micro-segmentation and provide L2-L7 security services.
- Virtual Security Control Module (vSCM) is the control panel, supporting policy configuration and distribution, as well as managing the lifecycle of the vSSM.
**Product Highlights**

- **Achieve Unparalleled Live Traffic Visibility:**
  All virtual machines’ access points can be monitored to provide visibility of traffic, applications and threats related to this 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 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 (ADI), 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 vSCM enables unified security policy configuration for each VM. CloudHive supports vMotion to ensure security services persist in the event the VM moves. Existing VM flows will not be interrupted by vMotion.

- **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 any upgrade or expansion of the current cloud platforms.

**Produc 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
- Real-time application database upgrade

**Visibility**
- Cloud asset auto discovery: networks and VMs
- Visualization of virtual network topology, VMs and traffic
- Deep insight and monitoring of all traffic between VMs
- Customized Visualization options: Sort, inquiry, filtering, zoom in/zoom out
- Log support: session logs, threat logs and system logs

**Firewall**
- Layer 2-Layer 7 access control
- VM and network based access control
- Time Table Based Access Control
- Application Layer Gateway (ALG)
- Session limit: New Session/Concurrent Session

**IPS**
- 7,000+ signatures, including custom signatures
- Predefined prevention configurations
- Protocol anomaly detection: HTTP, IMAP, POP, VOP, NETBIOS etc.
- 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**
- Defense against Malformed packet attacks
- DoS/DDoS defense: DNS Query Flood, SYN Flood etc.
- Defense against ARP attacks

**High Availability**
- Separation of management, control and service plane ensures the service stability
- vSSM “VM shutdown” does not affect the CloudHive service
- vSCM are deployed in pairs (Active/Passive) to provide high availability
- Single vSSM “VM down” does not affect the system, the user VM traffic can bypass the vSSM,
- vSCM can reboot and restart security service automatically after “VM down”.
- vMotion support: security policy and flow sessions automatically synchronize across multiple service modules
- Support in Service Software Upgrade (SSSU)

**Scalability and Automation**
- vSSM can scale up without interrupting security service, up to 200 vSSM modules
- Achieve VM based policy configuration through automatic learning on virtual assets.
- Detect VM up or down, and update VM IP change automatically

**Deployment**
- Support both tapping mode and transparent in-line mode
- L2 deployment without the need for network configuration changes
- Ease of deployment without root authority and any plug-in, minimized affect to VM and hypervisor.
- Enable or disable security service on VM or network through one click
- Support VSS/VDS, vSAN, NSX deployment
- Support 5G high speed with one vSSM module and VMXNET3 VM network card
- Support vCenter 5.0/5.1/5.5/6.0

**Management**
- Interface: RESTful API, CLI, WebUI
- Centralized and unified management through a single interface

**Hypervisor Compatibility**
- VMware vsphere 5.0/5.1/5.5/6.0

**Specifications**

Each of the three types of virtual modules that comprise CloudHive requires a VM with at least 2 vCPU cores, 4GB memory and 16TB Storage.

<table>
<thead>
<tr>
<th>Specification</th>
<th>CloudHive System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Throughput (Maximum)</td>
<td>1 Tbps</td>
</tr>
<tr>
<td>Maximum Concurrent Sessions</td>
<td>340 Million</td>
</tr>
<tr>
<td>New Sessions/S (HTTP)</td>
<td>6 Million</td>
</tr>
<tr>
<td>IPS Throughput (Maximum)</td>
<td>200 Gbps</td>
</tr>
<tr>
<td>vSSM Scalability (Maximum)</td>
<td>200</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Specification</th>
<th>Each vSSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Throughput</td>
<td>5 Gbps</td>
</tr>
<tr>
<td>Maximum Concurrent Sessions</td>
<td>1.7 Million</td>
</tr>
<tr>
<td>New Sessions/S (HTTP)</td>
<td>30,000</td>
</tr>
<tr>
<td>IPS Throughput</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

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

Version: EX-08.81-CloudHive-V2.2-0916-EN-01

www.hillstonenet.com