Hillstone™
NETWORKS

Hillstone CloudHive: Micro-Segmentation Security for Virtualized Data Centers

www.hillstonenet.com

As datacenters have evolved from physical to virtual, enterprise to cloud, the security challenges they face have evolved as well. Some of the trends that have changed the nature of datacenter security include:

Multitenancy The days of a datacenter serving a single organization are fading fast. Today's virtual and cloud enabled data centers--whether private, public, community or hybrid--are more likely to serve several organizations, subsidiaries or departments. Examples include government agencies, healthcare organizations or other entities sharing a single community cloud or hundreds of unrelated organizations taking advantage of public cloud infrastructure and applications.

With multi-tenancy, an organization may be served by scores of virtual machines and applications that share not only the same datacenter but the same physical servers with other tenants. To prevent data breaches and the spread of malware from tenant to tenant, each organization's virtual infrastructure must be isolated and protected from that of the other organizations sharing the same cloud, network or server.

Multi-cloud The concept of the datacenter as a physical place has faded as organizations have extended infrastructure and applications across public, private, and multi-clouds. Today, even a single business process or application may depend on infrastructure and components that span multiple cloud services and cloud types.

North-South to East-West In the early physical days of the Internet datacenter, security was mostly about monitoring and securing traffic entering and exiting a well-defined network perimeter. Today, east-west traffic among virtual machines, Web services and applications sharing the same data center and physical servers is just as or more common, not only among different tenants but servers and components of a single Web based or other composite application. Without proper protection, threats to one component or Web service can easily infect the others.

SDN and NFV While virtualization was mostly about servers, applications and storage for many years, today the network has caught up, with network hardware morphing into virtual and software defined networks. Software based networks have obvious advantages in standardization, agility and mobility. Unfortunately, today's SDN and NFV solutions are often still catching up with the robust security of legacy network hardware developed over decades, security that was often difficult to configure and maintain.

Mobility and elasticity Virtualization has enabled the dynamic, endlessly elastic mobile data center, with virtual machines, storage and network resources deploying, expanding, contracting and migrating at will. Securing such a dynamic datacenter environment with fixed, appliance based solutions is not a viable strategy. It's possible to detour all VM-to-VM and tenant-to-tenant traffic through a fixed security solution, but such a strategy is inefficient, difficult to manage and bound to have a negative latency and application performance impact, slowing down the pace of business.

The challenge that comes out of all these trends is how to insert security functions deeply into such a shared, virtualized, dynamic, elastic environment.

What Is Needed for True Cloud Security

The virtual cloud-enabled data center needs a new security strategy and solution that can cope with virtual demands with minimal performance impact. Such a solution must offer the following capabilities:

A virtual/cloud enabled solution Any security solution must be as virtual, flexible and elastic as the infrastructure it serves. It should be hypervisor aware and able to insert itself deeply into the virtual environment, protecting communications among virtual resources as they deploy, grow, shrink and migrate across the datacenter. It should be tightly integrated with virtual and cloud management and orchestration platforms such as VMware vCenter and OpenStack, and hypervisors such as ESXi, and offer cloud friendly API's such as a RESTful API so that it can secure infrastructure and applications across a multi-cloud environment.

While management platforms such as vCenter allow IT to configure vLANs to segment different users and virtual machines, the configuration process is manual and tedious. Any virtual security solution must be able to isolate traffic quickly and easily in an automated fashion based on policy and constant change.

Comprehensive NS/EW visibility When security focused mostly on North-South traffic, in-network physical firewalls were a viable solution. A virtual, cloud based solution must have deep visibility and insight into all North-South and East-West traffic among virtual tenants and servers, including the virtual network, virtual machines, applications and the multi-cloud. It must have the tools to display all that information clearly and draw attention to abnormalities and potential security issues in a format that makes it easy for IT to detect and address them.

Scalability and mobility The mobile, highly elastic virtual datacenter needs a highly elastic, scalable, mobile security solution that binds policies to each and every VM, remaining with each as it is deployed, moved and migrated, without any impact on security or application performance.

Multifunction L2-L7 security As malware and data breaches grow increasingly sophisticated, hidden and able to bypass traditional security solutions, the days of security addressed by a single application, tool or capability have long passed. For a cloud security solution to be successful, it must leverage multiple security strategies and capabilities, including access control, application detection and firewalls, intrusion prevention and malware protection. The solution must be able to address all these capabilities with minimal performance impact.

Hillstone CloudHive

Hillstone CloudHive is an advanced security solution designed from the ground up for the demands of the virtual, multitenant, multi-cloud enabled datacenter. Using advanced microsegmentation and a standard cloud orchestration API, CloudHive inserts its monitoring and security capabilities deeply and seamlessly into the virtual environment. It monitors and addresses all north-south and east-west traffic to detect, isolate and eliminate malware, potential data breaches and other security issues before they can spread across VM's, tenants and virtual networks.

CloudHive scales its virtual security resources automatically exactly where and when they are needed, binding and enveloping all VMs as they're deployed, moved and migrated across the virtual datacenter and multi-cloud (Figure 1).

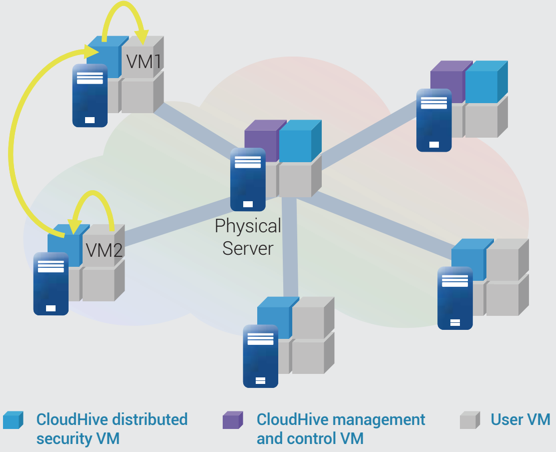
VM1
VM2
Physical Server
CloudHive distributed security VM
CloudHive management and control VM
User VM

Figure 1: Hillstone CloudHive Distributed Components

CloudHive's asset discovery creates a visual map of all datacenter and multi-cloud resources automatically, including virtual networks, virtual machines (VM), and all the connections among them. Its mapping capability presents IT with comprehensive views of all application traffic flows, traffic types and potential threats across VMs. Tight integration with existing cloud orchestration platforms such as VMware vCenter and OpenStack ensures rich, real-time contextual visibility across the multi-cloud and allows security resources to grow and shrink alongside the virtual resources to be secured.

CloudHive components are all VM- and software-based. To distribute and scale the security service in a flexible manner with minimal performance impact, the CloudHive architecture, shown in Figure 2, separates security functionality into three different planes.

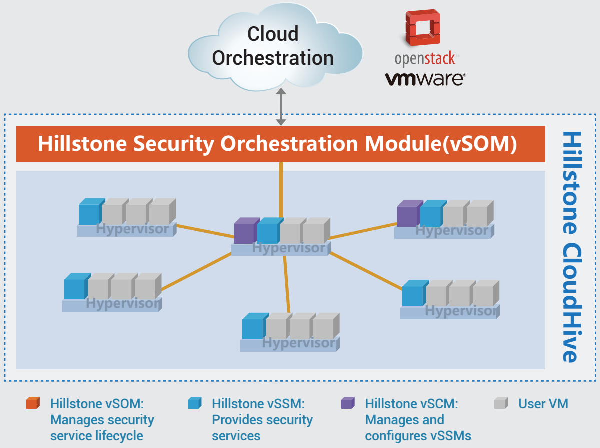
Cloud Orchestration
openstack
vmware
Hillstone Security Orchestration Module(vSOM)
Hypervisor
Hypervisor
Hypervisor
Hypervisor
Hypervisor
Hypervisor
Hillstone CloudHive
Hillstone vSOM: Manages security service lifecycle
Hillstone vSSM: Provides security services
Hillstone vSCM: Manages and configures vSSMs
User VM

Figure 2: Hillstone CloudHive Architecture

The security service plane is represented by CloudHive's virtual Security Service Modules (vSSM). CloudHive deploys vSSM's on each physical server to enforce advanced L2-7 security policy, manage sessions and scale elastically across all server VM's.

The control plane, represented by CloudHive's virtual Security Control Modules (vSCM), acts as the central security configuration manager, providing management interfaces (UI, CLI or RestAPI) to configure and monitor the virtual security service and manage the security policy configuration and lifecycle of all vSSM's. The control plane also collects and logs all security and traffic data.

The management plane, represented by CloudHive's virtual Security Orchestration Modules (vSOM), integrates and interacts with third-party cloud orchestration and administration tools to manage the service lifecycle of the entire CloudHive system, including system installation and starting, stopping, and deleting all components.

CloudHive Benefits

This three tiered architecture has several benefits:

Scalability and Mobility Separating management, control and security deployment allows each function to scale independently of the others, applying the precise level of each resource precisely where it is needed. Since all services are elastic and distributed throughout the virtual environment, they are always close to the virtual resources that they protect. This allows them to apply policy enforcement without the traffic detours bottlenecks that add latency and impact performance. CloudHive can apply security services on demand to any and all new workloads and VMs. vSCM deployment unifies security policy configuration across the multi-cloud.

The CloudHive control plane harnesses Hillstone's distributed architecture, vMotion awareness and a patented flow session distribution technology to maintain state as VMs grow, shrink and move across the multi-cloud without any security service interruption or delay.

Comprehensive visibility CloudHive's asset discovery feature builds a comprehensive display of cloud networks, VMs and virtual network traffic automatically, displaying all inbound and outbound traffic and highlighting communication paths, traffic types and trends on each path. CloudHive then offers live visibility and control of VM topology, east-west and north-south traffic, applications and inter-VM attacks. CloudHive's comprehensive visualization and logging allow enterprises and Cloud Service Providers (CSPs) to meet any and all compliance, security audit, policy review, and threat vulnerability analysis and remediation requirements.

Multifunction L2-7 security CloudHive protects all VM-bound traffic and inter-VM traffic with L2-L7 security services, including firewall features such as policy control and session limits,Intrusion Prevention, Anti-Virus and Attack Defense (AD), and fine-grained application control. Real-time mitigation blocks, impedes or quarantines active attacks. vSSM's secure all VM directed traffic, both north-south and east-west, enabling 100% traffic security coverage and a zero attack surface.

Low Total Cost of Ownership CloudHive security services do not require an update to VMware's NSX and have no impact on existing network topology. Their ease of management demands few IT resources, reduces operational errors and improves overall efficiency.

CloudHive installs components in a non-disruptive manner, allowing security services to be added or removed simply by adding and removing VMs from security service (vSSMs) distributed across the physical servers.

IT can take advantage of either of two CloudHive deployment modes to ensure seamless deployment. TAP mode, which monitors traffic via mirroring, is completely non-intrusive but offers no policy enforcement. It can serve as a viable first step to provide IT with deep visibility into network resources and traffic flows via asset discovery, VM traffic monitoring, and logging. Transparent mode (or inline mode) can then be used as a later subsequent step to inspect traffic and enforce security policies.

The virtual cloud provides a raft of new security challenges that did not exist in the legacy physical data center environment. Hillstone CloudHive's distributed, virtual security solution provides unprecedented cloud asset and traffic visibility, reducing the datacenter threat surface to near-zero, and offers the dynamic deployment flexibility, elasticity, orchestration integration, business efficiency and cost effectiveness that today's virtual cloud environments require.

By inserting and integrating components deeply and seamlessly into the virtual environment, Hillstone CloudHive enables robust, dynamic, effective, scalable, efficient and non-intrusive security in the cloud.

Hillstone™
NETWORKS

How to contact Hillstone Networks

Americas: +1-408-508-6750 | SEA: +65-6678-7660

Europe: +420-721-125-070 | MEA: +971-4557-1493

Email: inquiry@Hillstonenet.com