The Hillstone Cloud Data Center FWaaS Security Solution — FWaaS For OpenStack

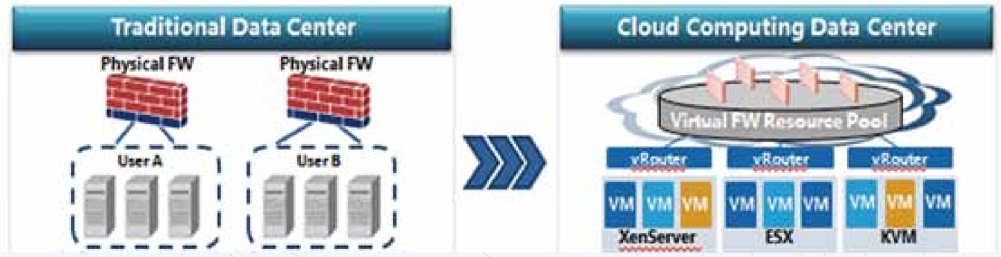
Overview

Traditional Data Centers transforming into Cloud Data Centers imposes challenges to traditional security architecture. The Hillstone Cloud Data Center (DC) Security Solution for Firewall-as-a-Service (FWaaS) provides protection for OpenStack-based public and private clouds such that tenants can use cloud services safely and securely by means of network isolation and policy protection.

The Hillstone Cloud DC Security Solution supports vsys virtual firewall services with dynamic allocation of firewall resources, elastic extension of hardware, and the ability to integrate with the main virtualization vendors. Managing this solution is simplified by using the OpenStack dashboard to administer the virtual firewall. The Hillstone Cloud Security Solution protects the cloud platform and ensures business continuity – the solution is suitable for carriers, Internet Service Providers (ISPs), Internet Content Providers (ICPs), industry business parks and many others types of businesses.

Security Challenges in Cloud Data Centers

The traditional DC provides a hosting service for physical servers – as such the boundaries of the service are clearly defined, and customers can deploy independent security appliances for servers as required. On the other hand, a Cloud DC provides a VM renting service where physical boundaries no longer exist, tenants no longer own physical devices, and therefore independent hardware security appliances can no longer be deployed for protection. A Cloud DC therefore requires a tenant FWaaS service in addition to virtual server rental.



Boundaries are clearly defined – customers can deploy independent security appliances

As boundaries disappear, tenants can no longer deploy independent security appliances for their servers

Figure 1: Traditional Network Security Solutions Are Unable To Adapt To Data Center Virtualization

FWaaS Service Using The OpenStack Platform

OpenStack is an infrastructure orchestration platform for public and private cloud services which helps build and manage IaaS services. The Neutron network component of OpenStack provides virtual network functions. Using the OpenStack virtual network functions, a physical firewall can provide virtual FWaaS for cloud tenants.

Hillstone Cloud DC FWaaS Solution

Hillstone provides an FWaaS Solution on the Hillstone X-series DC Firewall by using the Neutron virtual network component of the OpenStack platform. This solution helps Cloud service providers build FWaaS services into their Cloud DC offerings.

The Hillstone Solution software is installed via the OpenStack console as a Neutron vRouter component. When a tenant creates a vRouter in the OpenStack dashboard, the OpenStack console automatically connects to the Hillstone physical device to allocate a virtual firewall to the tenant, and to apply thesecurity policies based on the requirements entered. Each tenant can have one or more VLANs, while tenants are isolated from one another by self-owned virtual firewalls. Multiple virtual firewalls can share one physical I/O port – per tenant network traffic accesses the virtual firewall by host routing mode, and tenants can manage their self-owned virtual firewalls to configure dedicated security policies.

The Hillstone virtual firewall (vsys) supports SNAT, DNAT, server load balancing, IPSec VPN, application-based access control, anti-DDoS, session limits and many other features.

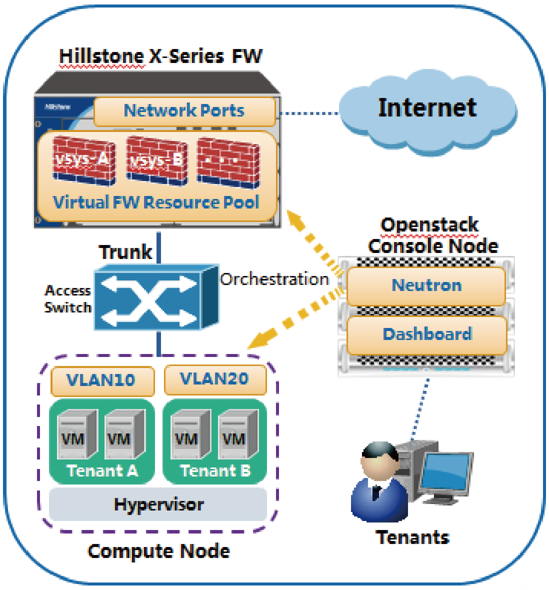


Figure 2: The Hillstone FWaaS Solution Architecture

Solution Deployment

In a public cloud data center architecture, with L2 data packets forwarded by the core switch, the Hillstone physical firewall is deployed as a hanging device bypassing the core switch. Two Hillstone devices work together in HA mode. For tenants renting a virtual firewall, the gateway function is removed, thereby enabling the virtual firewall to protect the tenant's VMs when these VMs and Internet users access each other. For tenants who do not rent a virtual firewall, the gateway function remains on the core switch, and the tenant's VMs and Internet users access each other directly, bypassing the firewall device.

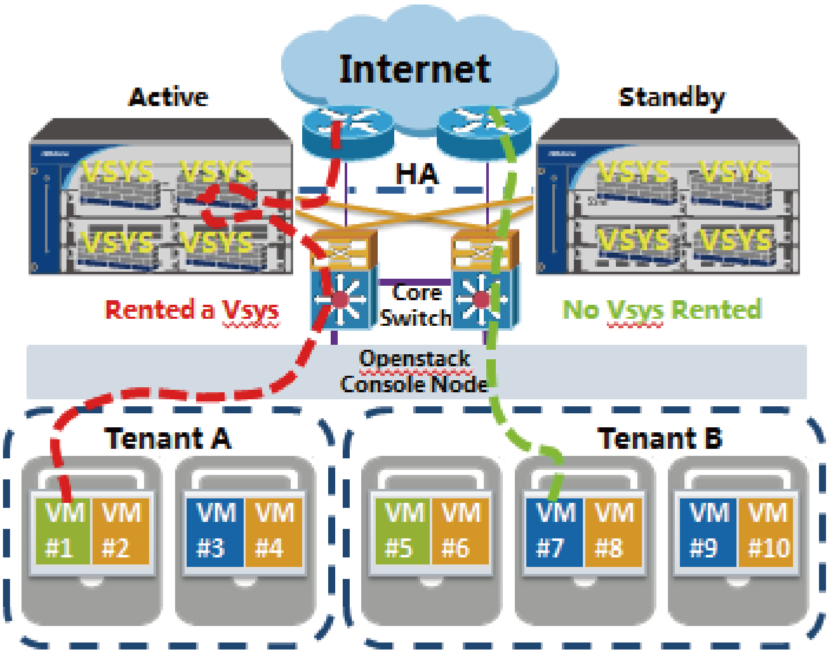


Figure 3: Hillstone FWaaS Solution Deployment

Solution Value

Convenient Deployment and Simplified Management

The Hillstone Cloud DC FWaaS Solution provides an independent virtual firewall for each tenant in the OpenStack environment, thereby implementing security protection for all tenants. All virtual firewalls can be configured and managed by the unified OpenStack platform. In a traditional DC, the administrator has to maintain every security device individually and separately. The centralized management offered by the OpenStack environment allows security device maintenance to become significantly more convenient. This solution supports the display of a graphical topology of the cloud network, and the administrator can easily understand the operating status of all security devices at the same time.

Dedicated Security Protection of All Tenants

In a Cloud DC, security requirements depend on each tenant's type of business, which is typically different for each tenant. The Hillstone physical firewall can be partitioned into multiple virtual firewalls by vsys technology – each virtual firewall flexibly deploys dedicated security policy based on the tenant's unique requirements. Tenants manage their own individual system resources, administration functions, security domains and policies independent from each other. When a virtual firewall is created, a tenant administrator can flexibly control traffic throughput depending on actual traffic observed by the tenant.

High Performance and Cost-Effective Security

The Hillstone FWaaS solution is based on a physical firewall with high reliability and stability. Virtual firewalls are isolated from each other – when a virtual firewall is attacked or encounters resource depletion, other virtual firewalls continue to operate normally and guarantees availability and business continuity of all tenants' services. In a Cloud DC, the advantage of firewall hardware deployment is that every virtual firewall provides the same high performance by dedicated security services without impacting cloud compute resources.

Enhanced Resource Utilization Through Elastic Expansion

The Hillstone FWaaS solution builds a virtual firewall pool for the Cloud DC. With the elastic expansion feature, tenants can dynamically create or delete virtual firewalls according to serviceneeds, with the result that the Data Center no longer needs to add more hardware. The Hillstone FWaaS solution enables deployment on demand, dynamic virtual firewall allocation, and elastic expansion in the Cloud DC – these features maximize resource utilization， compared to a traditional security solution, the Hillstone FWaaS solution requires less hardware deployment, and reduces Cloud DC infrastructure cost.

Summary

Users can deploy a public or private cloud, an industrial park cloud, or a hybrid cloud by using the OpenStack platform. The Hillstone FWaaS Security Solution on the OpenStack platform provides different cloud deployment options for Carriers, ISPs, ICPs, industrial parks, educational customers and many others. Compared with a traditional DC firewall, the Hillstone FWaaS Security Solution provides enhanced protection, performance and deployment flexibility, and is therefore highly suitable to Cloud DCs. The Hillstone FWaaS Security Solution provides comprehensive security protection and optimizes management and administration to provide simplified management of cloud security to users.

Hillstone X7180 Data Center Firewall

The Hillstone X7180 Data Center Firewall offers outstanding performance, reliability, and scalability for high-speed service providers, large enterprises and carrier networks. It provides flexible firewall security for multi-tenant cloud-based FWaaS environments. The X7180 platform offers highly scalable virtual firewalls (vsys), exceptional throughput, and massive quantities of concurrent sessions and new sessions per second. The X7180 also supports Deep Packet Inspection (DPI), next generation application control and Quality of Service (QoS). The system delivers exceptional performance in a small form factor with low power requirements.

Specification	SG-6000-X7180
	Front Rear
FW Throughput (Maximum)	360Gbps
Maximum Concurrent Sessions	120 million
New Sessions/s (HTTP)	2.4 million per second
Available Slots for Extensible Modules	10 x Generic Slot, 2 x System Control Module Slot, 1 x SD Card Slot
Maximum Power Consumption	2+2 redundant power supply, Max 1300W
Dimension (WxDxH)	5U 17.3×23.2×8.9 in (440×590×225 mm)