Huawei USG6000V Virtual Service Gateway

With wide application of cloud computing technology, IT and CT are rapidly converged. Consequently, requirements for public and private cloud deployment, quick service provisioning, on-demand service migration, and tailored attack defense increase sharply. Conventional service gateways with dedicated hardware can hardly meet the deployment requirements of the cloud network architecture.

Huawei USG6000V is a virtual (software-based) service gateway based on the network functions virtualization (NFV). It features high virtual resource usage because the virtualization technology allows a large number of tenants to concurrently use the resources. In addition, the USG6000V provides abundant virtualized gateway services, such as vFW, vIPsec, vLB, vIPS, vAV, and vURL Remote Query. It can be flexibly deployed to meet service requirements.

Huawei USG6000V series virtual service gateway is compatible with most of mainstream virtual platforms. It provides standard application platform interfaces (APIs), together with the OpenStack cloud platform, SDN Controller, and MANO to achieve intelligent solutions for cloud security. It meets the requirements of flexible service customization, elastic and on-demand resource allocation, visualized network management, rapid rollout and frequent changes of security service, and simple and efficient O&M.

Highlights

Integrated functions and fine-grained management

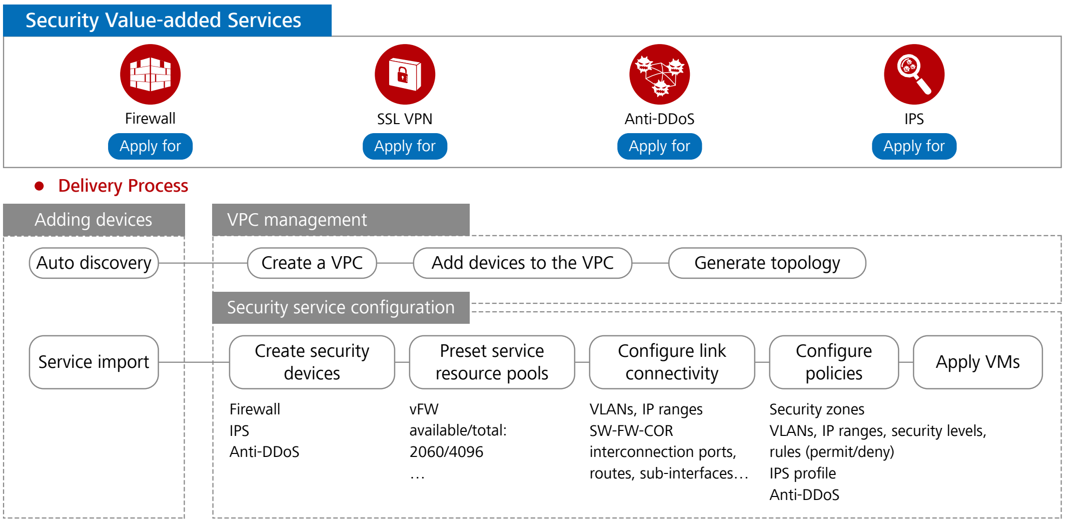
The USG6000V provides multiple functions, including security protection to data centers at the virtualization layer and value-added security services for tenants.

- **Multi-purpose:** The USG6000V integrates the traditional firewall, VPN, intrusion prevention, antivirus, data leak prevention, bandwidth management, and online behavior management functions all in one device, simplifying device deployment and improving management efficiency.
- **IPS:** The USG6000V can detect and defend against over 5000 vulnerabilities. It can identify and defend against web application attacks, such as cross-site scripting and SQL injection attacks.
- **Antivirus:** The high-performance antivirus engine of the USG6000V can defend against over five million viruses and Trojan horse. The virus signature database is updated daily.
- **Anti-DDoS:** The USG6000V can identify and defend against over 5 million viruses and over 10 types of DDoS attacks, such as SYN flood and UDP flood attacks.
- **Online behavior management:** The USG6000V implements cloud-based URL category filtering to prevent threats caused by users' access to malicious websites and control users' online behavior, such as posting. The USG6000V has a predefined URL category database that contains over 85 million URLs. In addition, the USG6000V audits users' network access records, such as posting and FTP operations.

- **Secure interconnection:** The USG6000V supports various VPN features, such as IPsec, SSL, L2TP, MPLS, and GRE VPN to ensure high-availability and secure interconnection between enterprise headquarters and branch offices.
- **QoS management:** The USG6000V flexibly controls upper and lower traffic thresholds and implements policy-based routing and QoS marking by application. It supports QoS marking for URL categories. For example, the packets for accessing financial websites are assigned a higher priority.
- **Load balancing:** The USG6000V supports server load balancing. In a multi-egress scenario, the USG6000V can implement load balancing with the egresses for applications according to link quality, bandwidth, and weights.

Flexible deployments of services achieved by elastic and on-demand principles

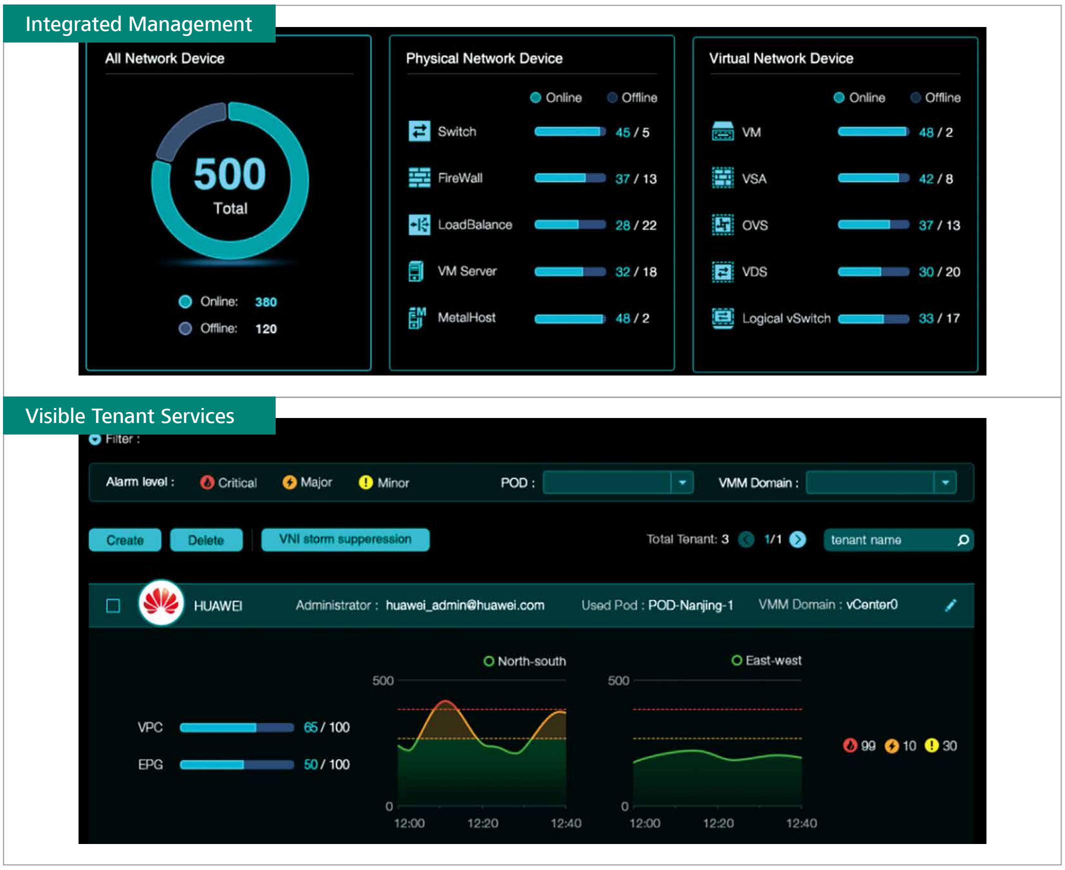
- **Virtualization:** The USG6000V supports the virtualization of many security services, such as firewall, intrusion prevention, antivirus, and VPN. Users can separately conduct personal managements on the same physical device. The USG6000V8 can be divided to 500 virtual systems to achieve one-to-many virtualization. It requires less investment from small-scale tenants by providing fine-grained service resources.
- **Automation:** It supports such plug-ins as NETCONF and OpenStack, and connects to Agile Controller or Openstack cloud platform through standard interfaces. With one-click configuration and delivery of network parameters on the portal, it spares users the nuisances of configuring complicated commands of specific network devices. It achieves seamless orchestration among computing, storage, and network by providing faster deployment of network resources. Network services roll out within minutes with manual configuration being reduced by 90%.



Service provisioning process of Huawei DCN security solution

Integrated management and visualized O&M

- **Security policy management:** Users configure security service rules based on security groups. The Agile Controller generates and automatically delivers security policies.
- **Visualized O&M:** It provides topology visibility for network-wide virtual and physical resources to quickly locate network fails. It also provides visualized network management based on tenants to meet compliance requirements of visualized network topology, quota, traffic, and alarms.



Online: 380
Offline: 120

Switch 45 / 5
FireWall 37 / 13
LoadBalance 28 / 22
VM Server 32 / 18
MetalHost 48 / 2

VM 48 / 2
VSA 42 / 8
OVS 37 / 13
VDS 30 / 20
Logical vSwitch 33 / 17

Total Tenant: 3 1/1

□ HUAWEI Administrator : huawei_admin@huawei.com Used Pod : POD-Nanjing-1 VMM Domain : vCenter0

VPC 65 / 100
EPG 50 / 100

99 10 30

Visualized Agile Controller management of Huawei DCN security solution

Building an ecosystem available to be integrated widely

By adopting standard APIs, it achieves zero transportation and zero cable layouts in the deployment of data centers. With this effortless deployment experience, it accelerates service deployments and supports migration among multiple virtual platforms. It provides automatic service scheduling and other functions by supporting comprehensive northbound interface protocols to realize wide connection to various kinds of standard controllers.

- **Various virtualization platforms:** Supports mainstream virtualization platforms, such as the VMware, KVM, XEN, and Huawei FusionSphere, as well as installation of bare machine.
- **Multiple file formats:** Supports software packages in multiple formats (including .vmdk, .iso, .qcow2, and .ovf) for deployment in various environments.
- **API friendliness:** Supports the management using NETCONF and RESTful NBIs and the OpenStack platform for NFV interconnection.
- **Solutions:** Supports solutions of Huawei DCN.
- **Public cloud platform:** Supports public cloud platforms of AWS and Huawei.

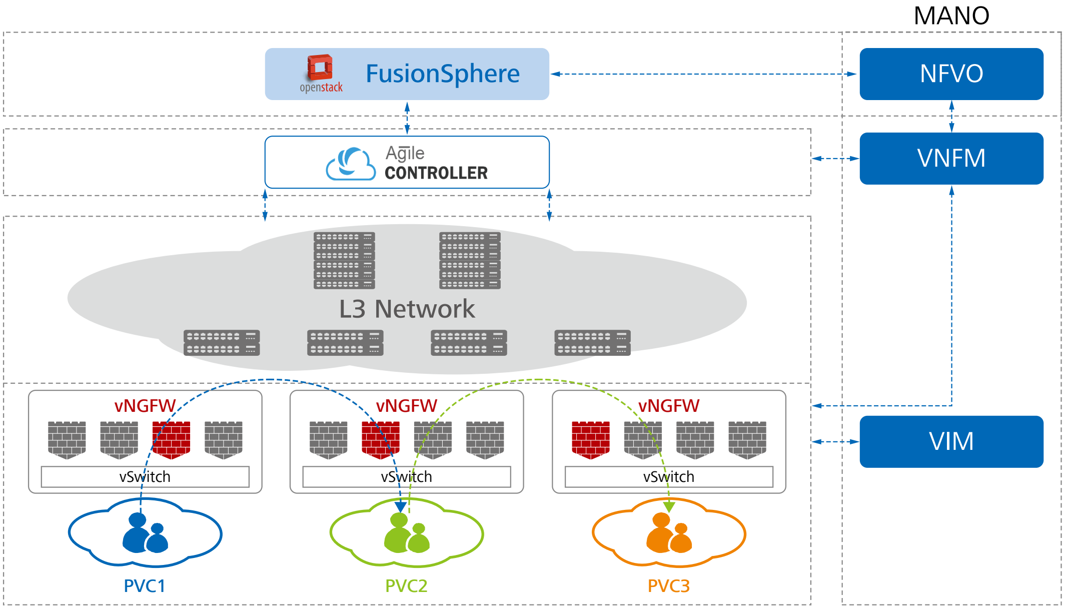
Typical Application Scenario

Huawei DCN security solution

Tenants subscribe to value-added services on the service portal; MANO deploys the USG6000V; the Agile Controller predefines the network and delivers security policies based on Layer 4 through 7. All of the procedures for rolling out the services are automated.

The USG6000V deployed on the border of the VPC of tenants provides such services as remote access, value-added security, and load balancing. It protects the north-south traffic among tenants from threat transmissions emanated from the data center.

The USG6000V supports as many as 500 virtual systems. It provides fine-grained security resources based on virtual systems to small-scale tenants, greatly lowering the threshold for investment.



Specifications

Model	USG6000V1	USG6000V2	USG6000V4	USG6000V8
Virtual Machine Resource Requirements[1]				
Hypervisor	Xen4.4 VMware ESXi 5.5 and above Linux KVM with kernel version 2.6.32 and above Huawei FusionSphere with kernel version 2.6.32 and above			
vCPU[2]	1	2	4	8
Memory (GB)	2 GB	4 GB	8 GB	12 GB
Storage (min/max)	2 GB/2 TB	2 GB/2 TB	2 GB/2 TB	2 GB/2 TB
Interface number of vNICs (min/max)	2/16	2/16	2/16	2/16
Main Performance[3]				
[SR-IOV mode][4] Firewall throughput[5] (1518-byte)	10 Gbit/s	20 Gbit/s	40 Gbit/s	80 Gbit/s
[SR-IOV mode] Number of new connections per second	15,000	30,000	100,000	280,000
[SR-IOV mode] Maximum number of concurrent connections	500,000	2,000,000	4,000,000	8,000,000

Model	USG6000V1	USG6000V2	USG6000V4	USG6000V8
[vSwitch mode][4] Firewall throughput[5] (1518-byte)	8 Gbit/s	8 Gbit/s	8 Gbit/s	8 Gbit/s
[vSwitch mode] Number of new connections per second	15,000	30,000	50,000	60,000
[vSwitch mode] Maximum number of concurrent connections	500,000	2,000,000	4,000,000	8,000,000
[SR-IOV mode] IPSec throughput[5] (AES, 1420-byte)	1.5 Gbit/s	2 Gbit/s	4 Gbit/s	7 Gbit/s
[vSwitch mode] IPSec throughput[5] (AES, 1420-byte)	1 Gbit/s	1.5 Gbit/s	3 Gbit/s	5 Gbit/s
Maximum number of IPSec connections	1,000	2,000	3,000	5,000
Maximum number of security policies	3,000	6,000	12,000	24,000
Number of virtual firewalls	20	50	200	500

Functions

Integrated protection	Integrates traditional firewall, VPN, intrusion prevention, antivirus, bandwidth management, and anti-DdoS functions.
Application identification and control	Identifies more than 6000 applications with the access control granularity to application functions, for example, distinguishing between WeChat text and voice. The USG6000V combines application identification with intrusion detection, antivirus, and data filtering, improving detection performance and accuracy.
Intrusion prevention and web attack defense	Accurately detects and defends against vulnerability-specific attacks based on up-to-date threat information. The USG6000V can defend against web-specific attacks, including SQL injection and XSS attacks.
Antivirus	Updates the antivirus signature database every day. The USG6000V can rapidly detect more than 5,000,000 types of viruses based on the signature database.
Bandwidth management and QoS optimization	Provides per-user or per-IP bandwidth management based on application identification, ensuring network quality for key services and users. The management and control can be implemented by maximum bandwidth, guaranteed bandwidth, application-specific PBR, and changing the forwarding priority of application traffic.
Load balancing	Supports Layer-7 service and link load balancing and fully uses computing resources based on abundant load balancing algorithms.

Model	USG6000V1	USG6000V2	USG6000V4	USG6000V8
Intelligent uplink selection	Supports service-specific PBR and intelligently selects the optimal link based on multiple types of load balancing algorithms (such as the bandwidth ratio and link health status) in multi-ISP scenarios.			
VPN encryption	Provides various reliable VPN features, such as IPsec VPN, L2TP VPN, MPLS VPN, and GRE.			
Anti-DDoS	Implements anti-DDoS to defense against over 10 types of DDoS attacks, such as SYN flood and UDP flood.			
User authentication	Supports multiple authentication methods, including local, RADIUS, HWTACACS, SecureID, AD, CA, LDAP, and Endpoint Security authentication.			
Security virtualization	Supports virtualization of multiple types of security services, including firewall, intrusion prevention, antivirus, and VPN services. Users can enjoy isolated and tailor-made management on one physical device.			
Diversified reports	Provides visualized and multi-dimensional report display by user, application, content, time, traffic, threat, or URL.			
Routing	Supports multiple types of routing protocols and features, such as RIP, OSPF, BGP, IS-IS, IPv6RD, and ACL6, in IPv4 and IPv6 environments.			
HA	Supports the active/active and active/standby working modes.			
Virtual network	Supports VXLAN Layer-3 gateways and Agile Controller VM awareness.			
Platform compatibility	Supports mainstream virtualization platforms, including VMware ESXi, Linux KVM, and Huawei FusionSphere.			
Software package format	Supports software packages in .vmdk, .iso, .qcow2, and .ovf formats for simple deployment.			

1. VM resources refer to resources provided by deployed VMs, including vCPUs, memory, hard disks, and virtual interfaces.
2. The vCPU indicates the logical CPU virtualized by the Intel x86 64-bit CPU that supports VT. One core corresponds to two vCPUs.
3. All performance indicators are tested under the specified hardware environment, namely, RH2288, V3, X86 series-3200MHz-1.8V-64bit-135000mW-Haswell EP Xeon E5-2667 v3-8Core-with heatsink.
4. In SR-IOV mode, the SR-IOV technology is used, and the test environment is the KVM platform. In vSwitch mode, the USG6000V is connected to the vSwitch, and the test environment is the VMware platform.
5. The maximum throughput is obtained by testing 1518-byte or 1420-byte packets in ideal conditions. The specifications may vary depending on live network environments.

Ordering Guide

Model	Description
Base Software	
Base Software License (Perpetual)	
USG6000V	USG6000V Basic Software License(per vCPU, 1 vCPU indicates V1, 2 vCPUs indicate V2, 4 vCPUs indicate V4, 8 vCPUs indicate V8)

Model	Description
Basic Software Subscription and Support	
USG6000V-1YSNS	USG6000V Basic Software Subscription and Support 1 Year(per vCPU)
USG6000V-3YSNS	USG6000V Basic Software Subscription and Support 3 Years(per vCPU)
Software Feature	
IPS Feature	
USG6000V-IPS	USG6000V IPS License(per vCPU)
USG6000V-IPS-1YSNS	USG6000V IPS Subscription and Support 1 Year(per vCPU)
USG6000V-IPS-3YSNS	USG6000V IPS Subscription and Support 3 Years(per vCPU)
AV Feature	
USG6000V-AV	USG6000V Anti-Virus License(per vCPU)
USG6000V-AV-1YSNS	USG6000V Anti-Virus Subscription and Support 1 Year(per vCPU)
USG6000V-AV-3YSNS	USG6000V Anti-Virus Subscription and Support 3 Years(per vCPU)
URL Remote Query Feature	
USG6000V-URL	USG6000V URL Remote Query License(per vCPU)
USG6000V-URL-1YSNS	USG6000V URL Remote Query Subscription and Support 1 Year(per vCPU)
USG6000V-URL-3YSNS	USG6000V URL Remote Query Subscription and Support 3 Years(per vCPU)
Content Security Group Feature	
CONTENT LIC	Content Security Group License (per vCPU or per V0)
Hardware	
IQA89501G1P5	PCIe Acceleration Card-Intel