



Huawei USG6000V Virtual Integrated Service Gateway

Product Overview

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

The USG6000V virtual integrated service gateway provides various gateway service capabilities, such as vFW, vIPsec, vLB, vIPS, vAV, and vURL filtering. All security functions are virtualized. Multiple tenants can share virtual resources. Therefore, you can deploy USG6000Vs flexibly based on tenants' demands, meeting the security compliance requirements.

Product Highlights

One device with multiple functions for accurate management and control

- One device provides multiple functions, including firewall, VPN, routing, load balancing, intrusion prevention, antivirus, and URL filtering, simplifies management, and improves resource usage.
- Detect increasing application-layer threats based on combinations of applications, content, time, users, threats, and locations for precise attack defense.
- Provide refined bandwidth management and guarantees bandwidth for key services based on applications and website categories, so that key services can be preferentially forwarded, improving user experience.

On-demand elasticity, flexible service deployment

- Tenants order services on demand. Resources are dynamically loaded

and reclaimed, making resource allocation flexible and elastic.

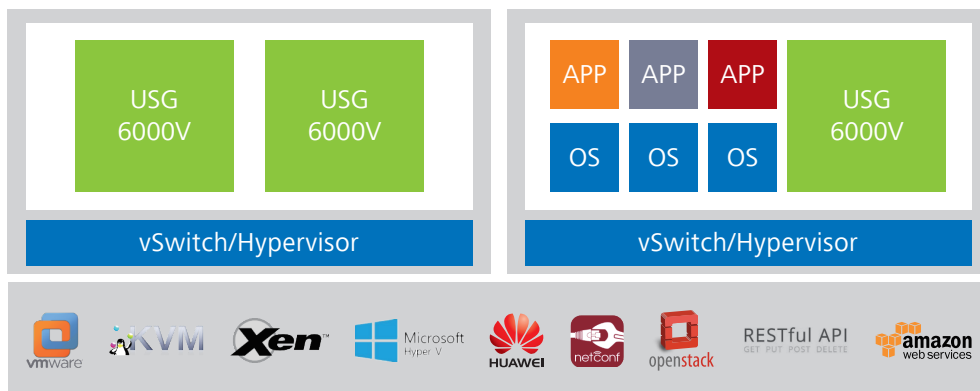
- Self-help tenant service configuration and automated provisioning reduce 90% of manual configuration workloads, launching services within minutes.
- Layer 2 through 7 security services are virtualized and can be flexibly orchestrated, meeting the diverse requirements of tenants in different scenarios.
- A physical resource can be virtualized into multiple virtual resources (virtual systems). Tenant resources can be allocated based on virtual systems in a refined manner, reducing network construction costs.

Unified management, visible O&M

- Physical and virtual resources are managed in a unified manner. Policies are managed based on security groups, and security policies can be automatically generated and delivered.
- The solution provides a topology for mappings between virtual resources and physical resources on the network, allowing rapid location of network faults and reducing management complexity.
- The solution provides a tenant-based network virtualization management view, which gives visibility into the network topology, quotas, traffic, and alarms of tenants, meeting compliance requirements.

Ecosystem building, being widely integrated

- Be compatible with mainstream virtual platforms VMware, Linux KVM, XEN, Hyper-V, and Huawei FusionSphere, and support bare-metal host installation.
- Support NETCONF and RESTCONF northbound APIs, programmable on the SDN controller for quick provisioning of new services. Support the OpenStack plug-in for management through a third-party OpenStack cloud management platform.
- Support Huawei DCN solution. Support AWS public cloud, Azure public cloud and Huawei public cloud.



Huawei USG6000V

Virtual Integrated Service Gateway

Detailed Product Specifications

Model	USG6000V1	USG6000V2	USG6000V4	USG6000V8
Virtual Machine Resource Requirements¹				
Hypervisor	Xen 4.5 and above VMware ESXi 5.5 and above Linux KVM, kernel 2.6.32 and above Hyper-V windows server 2012 and above Huawei FusionSphere 6.0 and above			
vCPU ²	1	2	4	8
Memory (GB)	2 GB	4 GB	8 GB	12 GB
Storage (min/max)	4 GB/2 TB	4 GB/2 TB	4 GB/2 TB	4 GB/2 TB
Interface number of vNICs (min/max)	2/11	2/11	2/11	2/11
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.			
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 IPv4 static routes, policy-based routing, routing policies, multicast, RIP, OSPF, BGP, and IS-IS. Supports IPv6 static routes, policy-based routing, routing policies, RIPng, OSPFv3, BGP4+, and IPv6 IS-IS.			
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, Linux KVM, XEN, Hyper-V and Huawei FusionSphere.			
Software package format	Supports software packages in .vmdk, .iso, .qcow2, and .ovf formats for simple deployment.			

1: Virtual Machine Resource Requirements refer to the requirements for resources provided for deployed VMs. The requirements cover vCPU, memory, disk, and virtual interface resources.

2: vCPU refers to a logical CPU virtualized from an Intel x86 64-bit CPU that supports VT technology. One core corresponds to two vCPUs.