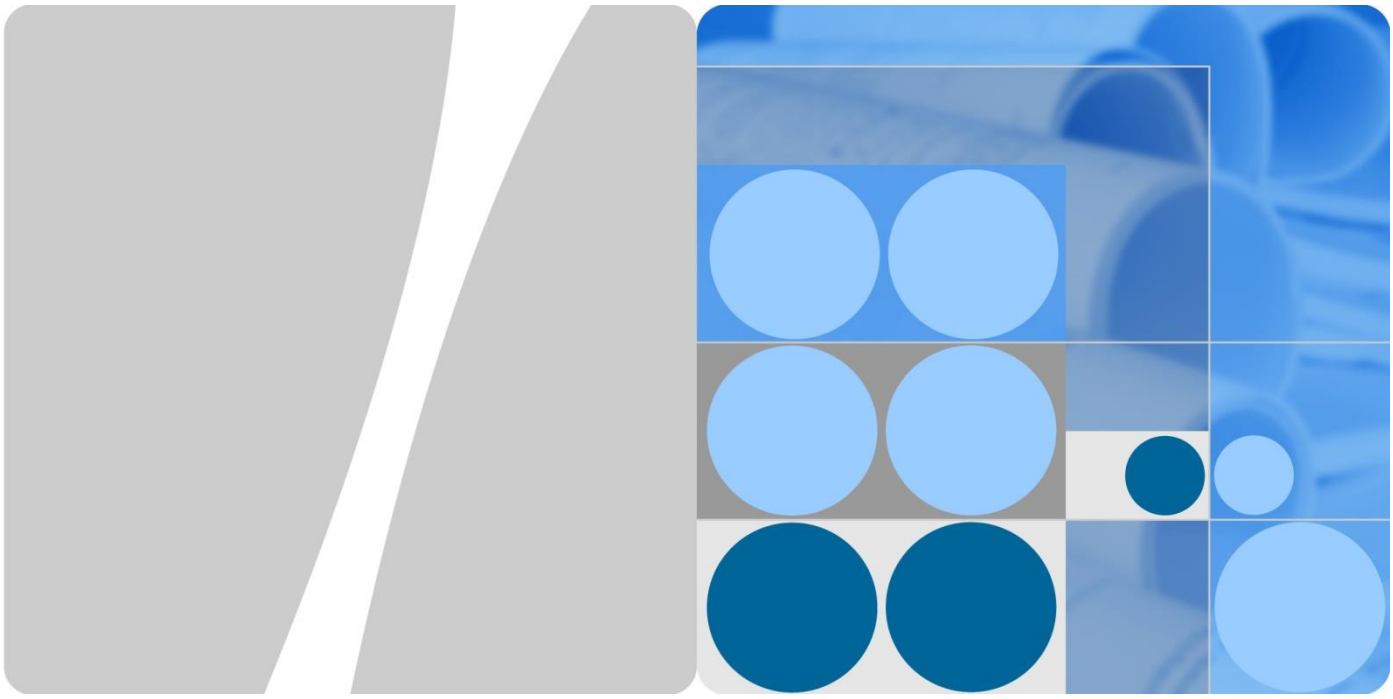


HUAWEI USG6000 Series Next-Generation Firewall Viatualization Technical White Paper

Issue V1.1

Date 2014-03-14

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. Please feel free to contact our local office or company headquarters.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 Technical Background 5

2 Basics and Operating Principle of Virtualization 6

2.1 Virtualization Basics 6

2.1.1 History of Virtualization 6

2.1.2 Network Virtualization and Its Development 7

2.2 Operating Principle of VFW 10

3 VFW Functionality and Services 13

3.1 VFW Management 13

3.1.1 Virtualization of Device Management 13

3.1.2 Resource Assignment and Withdrawal 13

3.1.3 Virtualization of the Feature Scanning Engine 14

3.2 Multi-Service Packet Forwarding 15

3.2.1 Diversified Traffic Distribution 15

3.2.2 Inter-VFW Packet Forwarding 16

4 Operation and Deployment 18

4.1 Networking Modes for Data Centers or Cloud Computing 18

4.2 Networking Modes for Intranet Isolation Among Enterprise Departments 19

Key Words

NGFW, VPN, virtualization, firewall, cloud computing, data center

Abstract

This technical white paper introduces the history and operating principle of virtualization, elaborates on virtualization implemented on Huawei firewall products (typically, USG6600), and draws prospects for virtualization.

Acronyms and Abbreviations

Acronym and Abbreviation	Full Spelling
ACL	Access Control List
AV	Anti-Virus
CAV	Chip-Assisted Virtualization
DLP	Data Leakage Prevention
GRE	General Route Encapsulation
IDC	Internet Data Center
IPS	Intrusion Prevention System
L2TP	Layer2 Tunnel Protocol
NAT	Network Address Translation
NGFW	Next Generation Firewall
SDN	Software-Defined Network
SSL	Secure Socket Layer
VFW	Virtual FireWall
VLAN	Virtual Local Area Network
VMM	Virtual Machine Monitor
VPN	Virtual Private Network

1 Technical Background

Even after a long time since its emergence, virtualization, which maximizes resource use efficiency by isolating and decoupling components or systems, has never been outdated. Innovations have propelled virtualization to advance along the path from the early virtual OS platform, virtual network monitor (VMM), virtual local zone network (VLAN), and virtual private network (VPN), to the prevailing Hipervisor, OpenFlow, and software-defined network (SDN). Virtualization has become a fundamental technology applied in the prosperous cloud computing industry and alike. Exuberant vitality has been seen in virtualization because it helps reduce CapEx and OpEx, and enables quick service integration.

New technologies represented by cloud computing have pushed the information technology (IT) industry over onto a tide of transformations. To embrace the revolutionary innovations and integration, Huawei has made a customer-oriented strategic realignment of "extending innovations from the telecommunication section to the enterprise and consumer service sections" with an attempt to build a service framework of "cloud – pipe – terminal". Under the big picture of service transformations, firewalls (FWs) also have to implement new prospective for virtualization, and final integration with the ocean-broad platform.

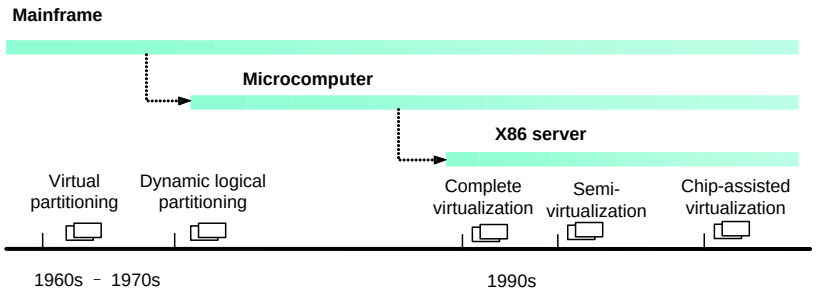
2 Basics and Operating Principle of Virtualization

2.1 Virtualization Basics

2.1.1 History of Virtualization

Virtualization is a logical expression of resources, regardless of their physical presence. A virtual system has a virtualization layer above physical resources.

Figure 2-1 History of virtualization



Virtualization originates from mainframes, with its earliest form of "virtual partitioning" traceable to the 1960s. It enables one mainframe to run multiple operating systems (OSs), and users to maximize the efficiency in using their expensive machines. Then technical advance along with marketing competition has transplanted "virtualization" onto microcomputer or UNIX server systems.

In the 1990s, virtualization software vendors designed a new software solution where a virtual machine monitor (VMM) virtualized the x86 server platform. This software-based virtualization solution has a limitation. That is, the VMM had to control and assign the essential platform resources to each guest OS, with a binary system conversion involved in the whole process. This conversion, however, required overheads that deteriorated the "complete virtualization" performance to an unacceptable extent. As a counter to this performance issue, "semi-virtualization" came into being. Unlike "complete virtualization", it did not need any binary system conversion, but changed guest OS codes instead. The changed guests OSs obtained extra performance and high scalability. To one's concern, guest OS code changes caused conflicts in system commands and low operating efficiency, which required uncountable workload in optimization to rectify. For now, virtualization has advanced to a new stage with hardware support. For example, chip-assisted virtualization (CAV) implements the functions of pure software virtualization using circuits. CAV reduces system overheads required for a VMM to run while addressing the needs of CPU semi-virtualization and binary system conversion. The virtualization-capable hardware simplifies VMM to a generic level. CAV empowers virtualized I/O while integrating virtualization-enabling

commands on processors, reaching the final goal of whole platform virtualization. Then a big picture of virtualization application unfolds ahead.

2.1.2 Network Virtualization and Its Development

Currently, the fast-changing client services require flexible network infrastructure that is easy to build and maintain. "Flexible" means that only logical changes are needed for providing varied network capabilities. Network virtualization is a typical example, which establishes logically-separated network environments on physical facilities to address diversified service needs while giving the users the experience of "separate and exclusive". Virtualization decouples logical expression from physical presence, and requires changes on a part, instead of in whole, for a physical network upgrade or logical network change.

The typical virtualization applications are VLAN, VPN, and virtual firewall (VFW) in being, and software-defined network (SDN) in future.

- VLAN: It is commonly applied on Layer 2 and Layer 3 switches, to resolve the broadcast zone issue. Users are classified into different broadcast zones so that they will not receive unwanted service packets. VLAN is an early form of network virtualization.
- VPN: It is a recently popularized technology that was dramatically developed with the wide application of Internet. It provides private network paths over a public network. In VPN, "virtual" means a logical expression of network. VPN ensures economic, effective, and secure connections between enterprise Intranets and users outside, or between enterprise branches.

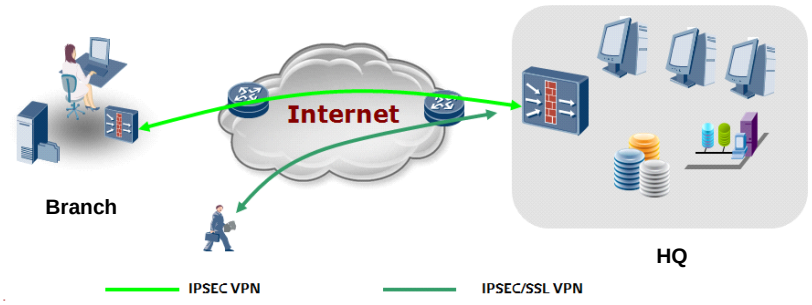
  As a basic operating principle, VPN uses tunneling technologies to encapsulate packets into tunnels and establish private data transmission tunnels on backbone networks to achieve transparent transmission of data packets. The tunneling technologies encapsulate one type of protocol packets using another protocol, which can also be further encapsulated or carried by other protocols.

  VPNs have the following advantages against the traditional private data transmission networks:

  - More secure: Secure connections are established between the headquarters and teleworkers, branches, partners, or suppliers to ensure data confidentiality. Secure connections are particularly important for e-commerce and the integration of financial networks and communications networks.
  - Less expensive (low-cost): VPN uses the shared public network instead of leasing private lines.
  - Better support for mobile services: VPN users can access the headquarters anytime and anywhere.

  VPN has been increasingly accepted by the enterprises that want to free up themselves from concerning about network operation and maintenance, and to concentrate on business achievements. VPN is highly flexible and scalable, while ensuring a high level of security, reliability, and manageability. It is available whenever there is Internet access.

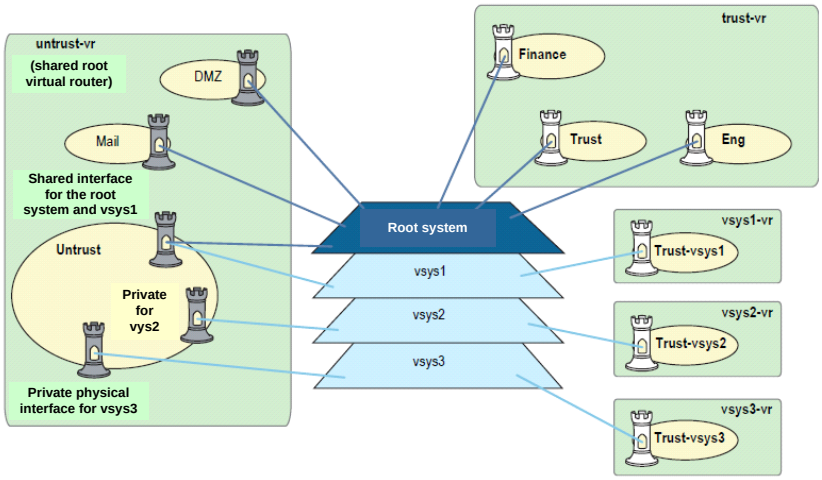
Figure 2-2 VPN application of Internet



Huawei next-generation firewall (NGFW) USG 6600 supports various VPNs, including IP security (IPSec) VPNs, Layer 2 tunneling protocol (L2TP) VPNs, generic routing encapsulation (GRE) VPNs, and secure socket layer (SSL) VPNs.

- VFW: One firewall system may be virtualized into multiple virtual systems. Each virtual system has its own administrator, who is allowed to set the address and service sets, manage users, and configure policies to address diversified security needs.

Figure 2-3 VFW



VFWs may be used for the following purposes:

- Device leasing: Small-sized enterprises can lease VFWs to protect their networks without paying for physical security devices, licenses, and after-sales services. Network operators can virtualize one physical FW device into multiple stand-alone systems to provide security assurance functions to enterprises while allowing them to share hardware resources but isolate their traffic.
- Network isolation: Medium and large-sized enterprise networks contain a large number of devices and require strict access permissions by network segment. Though traditional FWs can isolate networks by dividing them into security zones, the interface-based security zones may not meet the requirements on a complex network, and complex policy configurations are prone to errors. In addition,

administrators of multiple networks have the same permission on the same device, which easily causes configuration conflicts. In contrast, the virtual system technology can divide a network into independently-managed subnetworks, making network boundaries clearer and network management easier.

- Cloud computing: Cloud computing mainly stores network resources and computing capabilities in the cloud. Users can access the resources and services after they connect to the Internet. For the access, traffic isolation and security are important. The virtual system technology enables the FW deployed at the egress of the cloud computing center or data center, to isolate user traffic while providing security assurance.

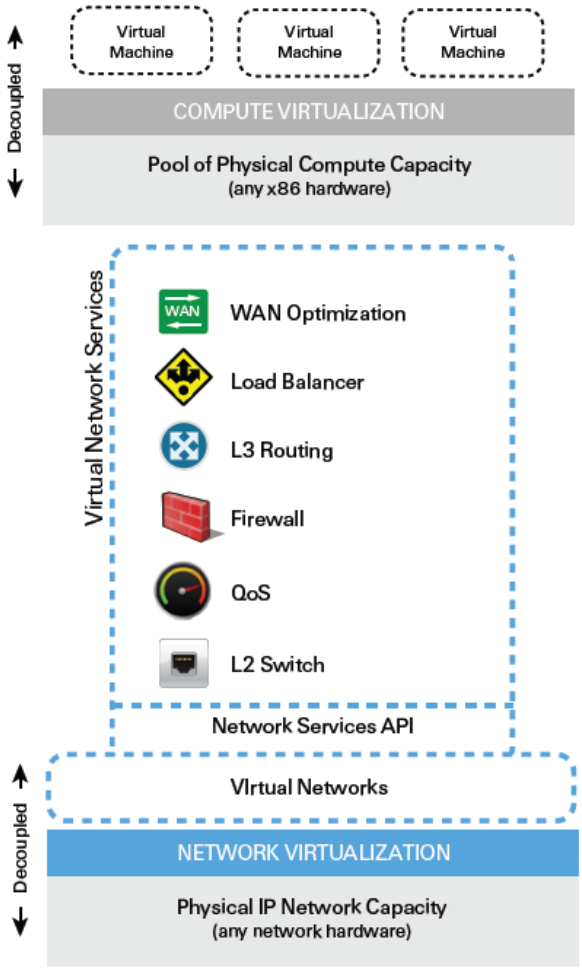
- SDN: It emerges out of cloud computing and has not come to the mature level for commercial use yet. Cloud computing service providers assign highly available and scalable IT resources on their clients' demands, for the purpose of computing, storage, or data transmission. Virtualization logically expresses physical resources while concealing the limitations on the physical level, and makes it possible to more accurately manage and apply the resources.

  Computing virtualization (mainly, x86 virtualization) has gained significant advance in recent years while virtualization in storage and network still has many issues to resolve, especially in cloud computing environment. Though OpenFlow and SDN did not come into being for network virtualization, the standardization and flexibility brought by them unfolds infinite possibilities for network virtualization.

  OpenFLow was proposed by the Stanford's Clean Slate Program, which attempted to enable network administrators to define security control policies specific to network flows using a centralized controller and to apply them to various network devices, to ultimately control the entire network security. Unlike traditional networks, OpenFlow separates the data plane from control plane on network devices and uses standardized interfaces on a controller to manage and configure network devices. This approach provides more possibilities for designing, managing, and using network resources, and propels network innovations and advance. OpenFlow means programmability on networks.

  The Program further proposed SDN based on OpenFlow. If network devices are resources under management, then a network OS can be abstracted according to how an OS works. This network OS logically expresses the physical network devices underneath while providing unified management views and programming interfaces for applications above. Then, on this network OS, users may develop application software to define the logical network topology and to address diversified needs of network resources without any need to concern about the underlying physical network's structure.

Figure 2-4 Future network virtualization - SDN



As cloud computing is advancing, FW will play an important role in SDN.

2.2 Operating Principle of VFW

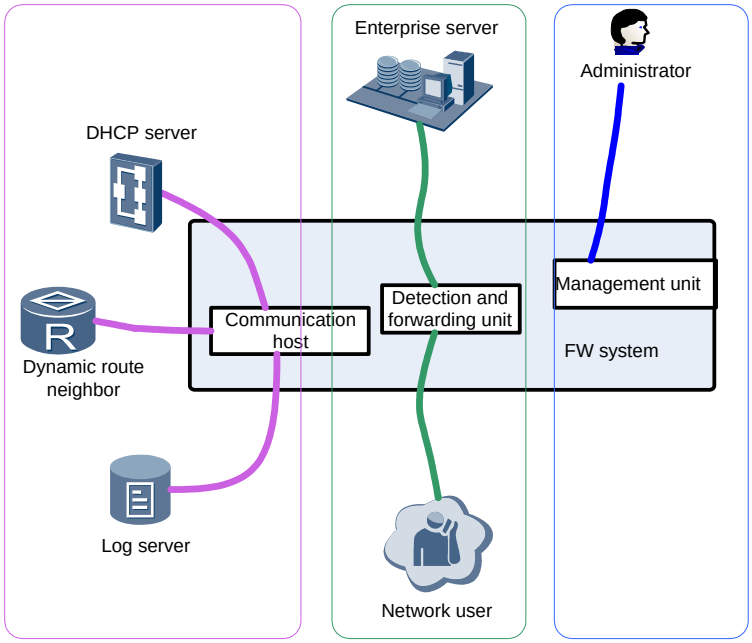
FW products serve as egress gateways for enterprise or campus networks, or data centers, and they isolate, filter, and detect traffic. FW has evolved through several generations from the earliest packet filtering to the latest content security assurance. The evolution also sees application of virtualization on FW, such as VLAN, VPN, and VFW in the past, and SDN in the future.

For now, Huawei FW products are NGFW-capable and their virtualization capabilities have come to the transition stage (transition from VPN-based, to VPN-free, and finally to VFW-operational). VFWs are logical FWs and have the same functions as physical ones.

Huawei medium and low-end FWs (USG series) now in sales are VPN-based and their virtualization is based on bindings of configurations to VPN instances. This approach requires complex configurations but leaves resource management far behind the need for independent management of virtual systems. Huawei NGFW USG6600 V100R001 releases VFW from VPN instance bindings by virtualizing most FW functions like virtual system

management, resource assurance and limitations, security policies, network address translation (NAT), static routes, and anti-DDoS.

Figure 2-5 FW ecosystem

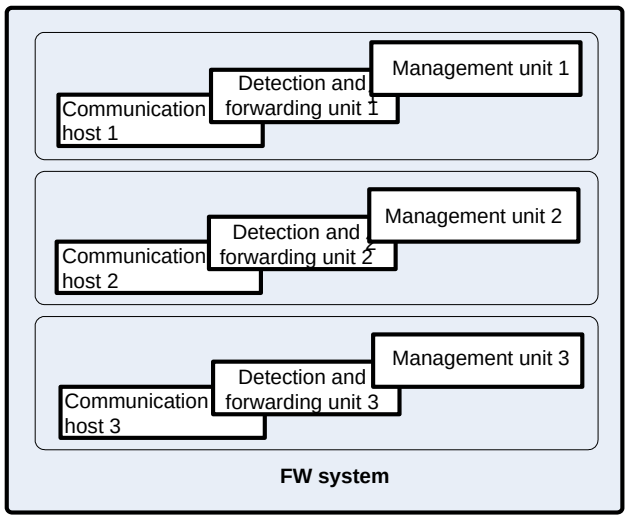


In an FW ecosystem, an FW has three roles to play: detection and forwarding unit, communication host, and management unit.

- Detection and forwarding unit: a forwarding system empowered with security detection functions.
- Communication host: It obtains an IP address and negotiates on the routing protocol and VPN passwords.
- Management unit: a manageable network element (NE).

After the physical FW is virtualized, each role has multiple virtual entities to play, as shown in the figure below. The entities with the same role are independent from each other, though they share physical resources. For example, the entities share the CPU and memory resources provided by the physical FW, or they implement communication and forwarding functions through the same interface. The following sections elaborate on the techniques used to duplicate roles among the logical entities.

Figure 2-6 Role duplication after virtualization



3 VFW Functionality and Services

3.1 VFW Management

3.1.1 Virtualization of Device Management

VFW is a logical and independent NE, but brings the same operating experience for administrators as a physical FW. Virtualization of management has the following issues to resolve:

- Separately storing configurations

  One configuration is used as usual and the configurations of one VFW are stored apart from those of another. Configurations of multiple VFWs are serially saved. VFW administrators can import or export configurations of only the VFWs under their charge.
- Separately applying feature configurations

  VFW IDs or mapping is used so that no name or ID conflict will occur. For example, a VFW ID is marked on IPS user-defined signatures.
- Isolating permissions of system administrators

  A VFW view is designed for separate VFW configuration and management. All VFW-associated configuration commands are put together in the VFW view. All these configuration commands are consistent with those that the root FW administrator sees in the system view, which means there is no need for extra parameters. Then an administrator can configure a VFW in the same way as configuring a physical FW. Moreover, VFW configurations are centralized for higher efficiency and easier check and management.
- Discretely recording logs and audits

  VFW information is added in all types of logs and audits. In addition, a stand-alone log server can also be configured for a VFW.

3.1.2 Resource Assignment and Withdrawal

VFWs share all the resources available on the entire physical FW. This resource sharing mechanism may lead to excessive resource usage on one VFW and resource shortage on another. A policy must be designed as a supplement to the resource sharing mechanism so that resources are certainly assigned for every VFW and the user efficiency is maximized among VFWs when some are vacant. The resources include CPU, memory, and interface resources. This policy must achieve the following purposes:

- Each VFW has resources available to use.

- No VFW shall occupy excessive resources.
- No VFW shall maliciously occupy resources while it does not need them, leaving a deny of service (DoS) vulnerability.
- Resources assigned for vacant VFWs shall be available to other VFWs that require them.

Such a policy will ensure proper assignment and use of resources. Specifically, a resource quota is specified for each VFW, defining the committed and peak resource levels. If the committed level is defined but the peak level is not, they are equal by default.

There are two general types of resources: stably-needed and dynamically-needed.

For stably-needed resources like the security policy count, address count, local user/user group count, NAT address/address pool count, and SSL VPN tunnel count, only a committed level is drawn. This approach simplifies the system.

VFWs apply for dynamically-needed resources based on data forwarding needs. For example, session tables, monitoring tables, and bandwidth on the forwarding plane are needed from time to time. A VFW may require few in one time and many or even all in another. To address the resource needs, the root FW administrator can specify a committed level and a peak level. This policy reserves some resources for VFWs to share, to content for. Then the entire FW resources are effectively used.

After VFWs are deleted, their resources are withdrawn and re-assigned for other VFWs.

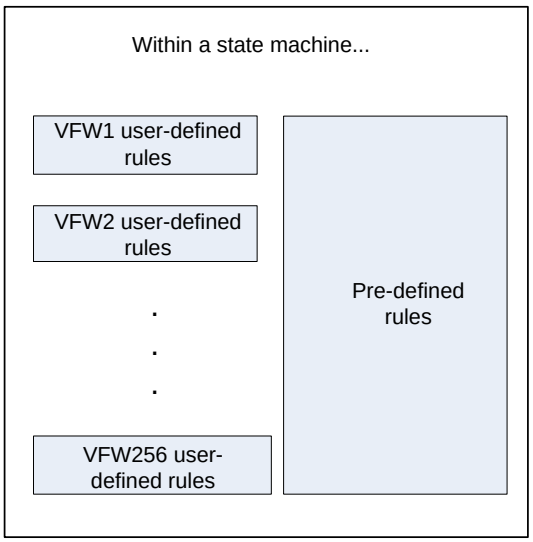
3.1.3 Virtualization of the Feature Scanning Engine

Content security functions like IPS, DLP, and AV are implemented by a feature scanning engine based on a state machine. Packet attack, virus, and threat files are expressed as one or more feature strings, officially-released or user-defined. These feature strings are compiled into state machines, against which packets are matched to identify threat fragments in packet content.

Virtualized security functions enable each administrator to define their own rules. These rules can be either packaged into a state machine, or separately saved, depending on the technical balance. If they are packaged, the state machine can include only consistent rules, and may be over-sized to poor performance. If they are saved separately, the state machines as many as VFMs are required, affecting performance, and packets have to be sent to the scanning engine repeatedly.

To keep a technical balance, rules specific to different VFWs are packaged into one state machine.

Figure 3-1 Virtualized feature scanning engine

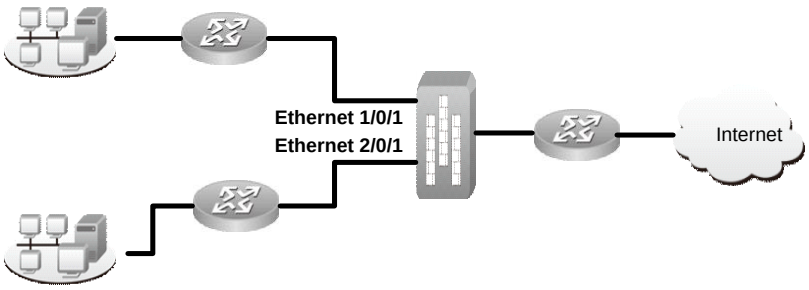


3.2 Multi-Service Packet Forwarding

3.2.1 Diversified Traffic Distribution

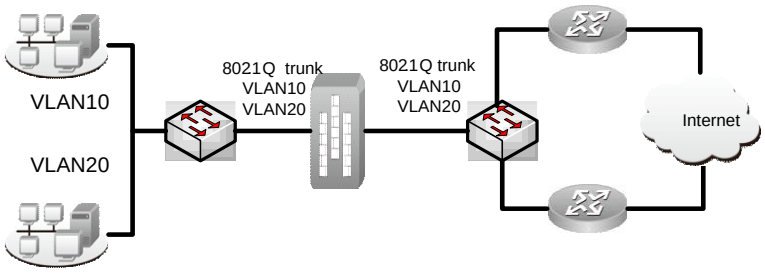
As shown in Figure 3-2, each VFW uses a stand-alone physical ingress and they share a physical egress. This approach applies when sufficient physical interfaces are available. Traffic distribution is easy to implement in this case. Specifically, stand-alone interfaces are bound to VFWs and traffic is distributed by ingress index to different VFWs.

Figure 3-2 VFWs connected to stand-alone physical interfaces



As shown in Figure 3-3, VFWs work in transparent mode. Specifically, enterprise networks are connected to an FW through VLANs and their traffic is distinguished by VLAN ID. A VFW is assigned for each VLAN and traffic is distributed to VFWs by VLAN.

Figure 3-3 VFW in transparent mode – by-VLAN traffic distribution

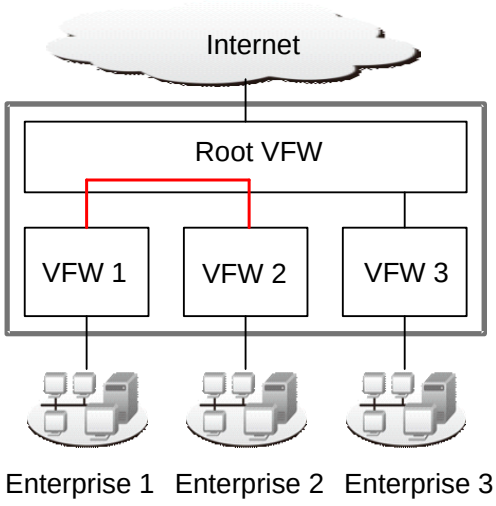


The VLAN interfaces must work in Trunk mode to receive VLAN-specific data packets. Then traffic is identified by VLAN ID. Data packets of VLAN 10 and VLAN 20 enter the FW, which distributes them to VFWs by VLAN ID.

3.2.2 Inter-VFW Packet Forwarding

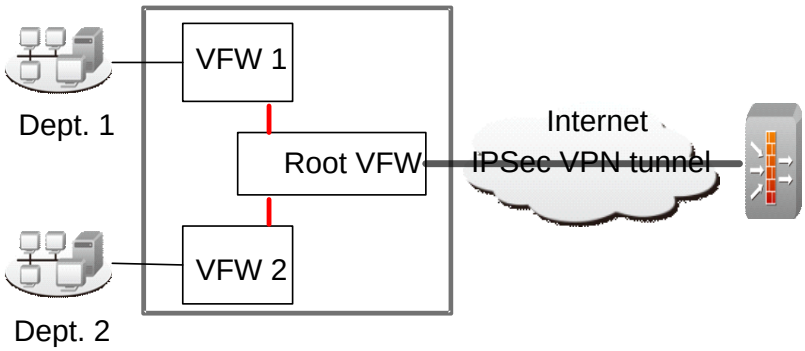
VFWs are assigned for different enterprises. Inter-VFW communication may be required for them to communicate with each other, as shown in Figure 3-4.

Figure 3-4 Inter-VFW packet forwarding



As shown in Figure 3-5, Dept. 1 and Dept. 2 need to communicate through VFWs, and the root VFW distributes the communication traffic. The root VFW also establishes a tunnel leading to the remote destination. Then the data packets of Dept.1 and Dept.2 are securely carried over the shared tunnel on the root VFW.

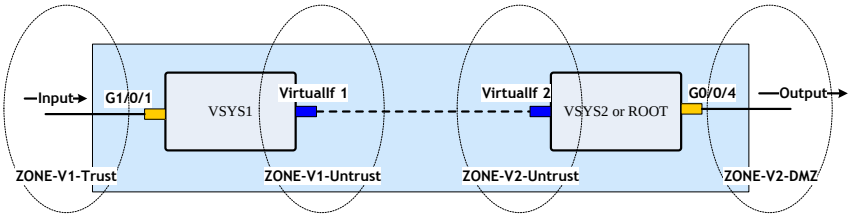
Figure 3-5 IPSec VPN on VFWs



For inter-VFW data forwarding, the physical FW has to forward to traffic inside, which is a technical issue to resolve. Interface virtualization is a solution to the issue. Then communication through VFWs is the same as that through physical FW.

As shown in Figure 3-6, VSYS1 receives and processes traffic, and then sends it to VSYS2, which can be the root VFW or an ordinary VFW. Each VFW has a virtual interface numbered VirtualIfxx, where xx indicates a VPN ID. Virtual interfaces can be included in any VFW security zone. In an inter-VFW data forwarding process, virtual interfaces distribute traffic and bridge security zones. In addition, virtual interfaces are effective only for inter-VFW forwarding.

Figure 3-6 Communication between virtual systems



4 Operation and Deployment

4.1 Networking Modes for Data Centers or Cloud Computing

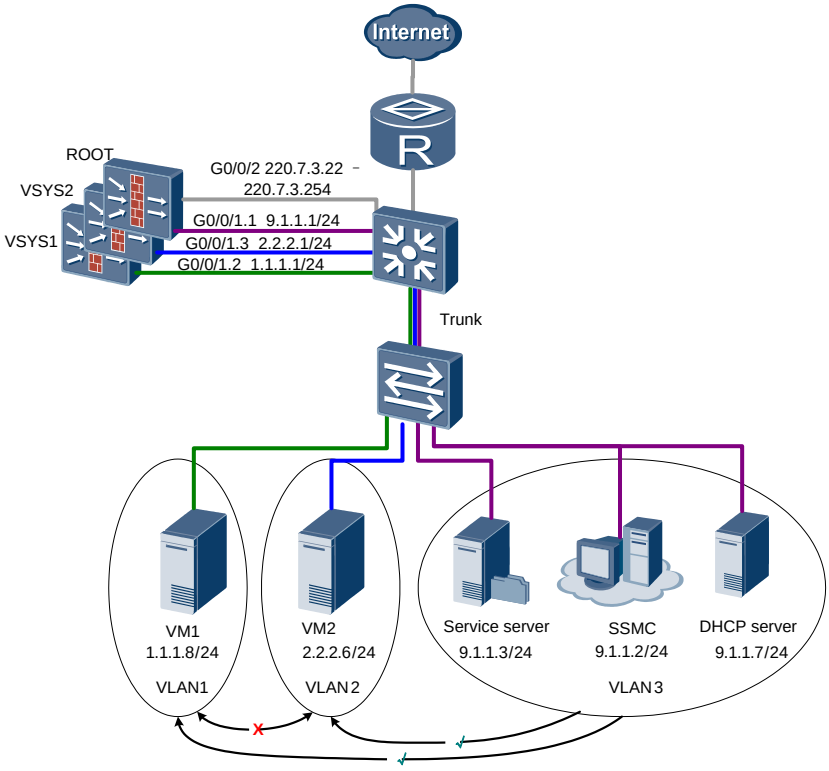
Data centers run a large variety of services and applications, and process and store data for them. Data center facilities include massive servers, disk arrays, security devices, and network devices, which together provide service access and carrying.

The cloud computing technology is used to store network resources and computing capabilities in the cloud. Users can access the resources and services after they connect to the Internet. A cloud can be seen as one or more virtualized data centers.

For data centers or cloud computing centers, traffic isolation and security are important. The virtual system technology enables the NGFW deployed at the egress of the cloud computing center or data center to isolate user traffic and provide security capabilities.

- A physical server may be virtualized into logical servers, or VMs, which provide services as servers usually do. A shared service management center (SSMC) manages the storage, server, IP, bandwidth, and network security facilities in a unified manner.
- VMs are isolated by VLAN, which means VLAN-specific VMs cannot communicate. Multiple VMs may be assigned for one VLAN. Service servers and SSMCs are free to access every VM.
- VFWs are the default gateways for VMs and they interconnect with Internet through a public network IP address or an IP address group.
- The SSMC monitors VFWs by running scripts and enables the administrator to configure security and bandwidth policies.

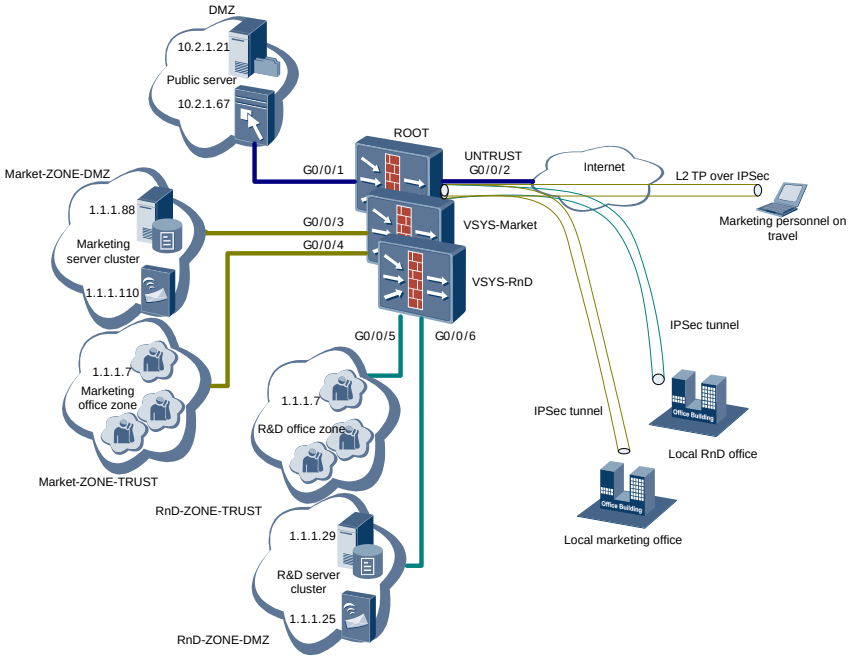
Figure 4-1 VFW application in data centers or cloud computing centers



4.2 Networking Modes for Intranet Isolation Among Enterprise Departments

Medium and large-sized enterprises' networks have massive network devices deployed. To protect information assets, network access permissions must be configured precisely for each network segment. Though traditional FWs can isolate networks by dividing them into security zones, the interface-based security zones may not meet the requirements on a complex network, and complex policy configurations are prone to errors. In addition, administrators of multiple networks have the same permission on the same device, which easily causes configuration conflicts. In contrast, the virtual system technology can divide a network into independently-managed subnetworks, making network boundaries clearer and network management easier.

Figure 4-2 VFW application for the traffic isolation purpose



As shown in the figure above, a large-sized enterprise network is divided into two zones: R&D and marketing. For security reasons, network traffic is restricted within each zone, or between each zone and Internet.

- Two VFWs, VSYS-Market and VSYS-RnD, isolate the two zones, which then cannot access each other, but both can access the shared servers.
- The network device IP addresses of one zone can repeat those in the other, which enables flexible networking.
- VSYS-Market and VSYS-RnD are managed by their IT administrators, who may configure respective policies for access authentication, security assurance, and bandwidth use. This approach makes network management clear.
- The root VFW administrator may assign resources, such as bandwidth, policy count, and session count, to other VFWs according to the department profile, including the headcount, and service model.
- The two zones connect to Internet by sharing interfaces on the root VFW.
- The enterprise branches connect to the server networks open to them by establishing an IPSec tunnel connected to the root VFW. The root VFW distinguishes packets by IPSec tunnels' SPI indexes and distributes traffic to other VFWs.
- Traveling marketing personnel may access the marketing server network over L2TP over IPSec tunnels connected to the root VFW. Then the root VFW distributes packets to VFWs by VPN instances that are bound to VT interfaces.