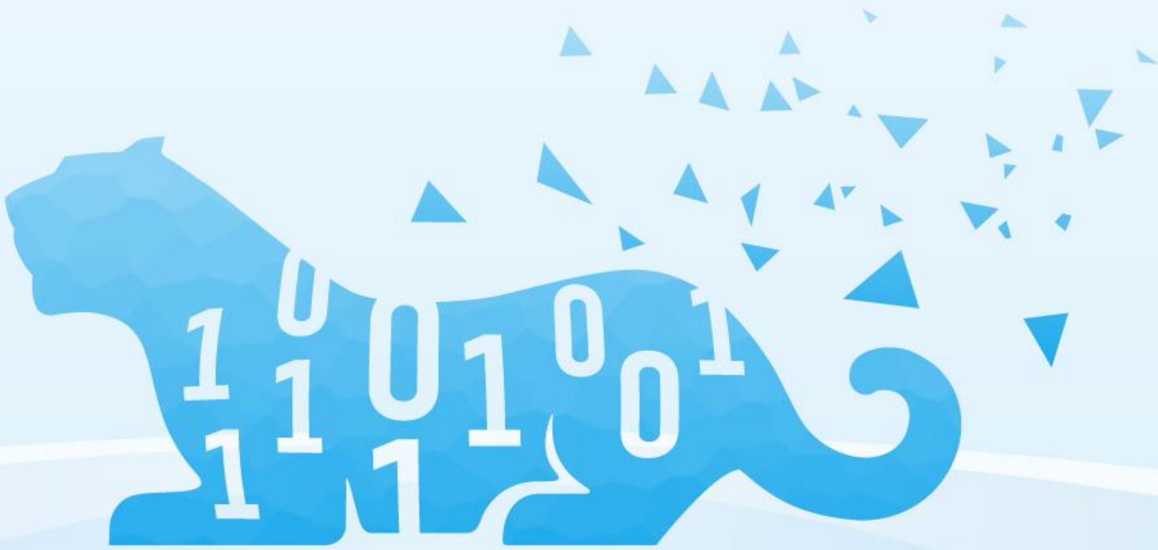
Legendsec Next-generation Firewall

White Paper



- Declaration

- Document Information

File Name	QAX Legendsec Next-generation Firewall White Paper		
Author		Date	
Version	V1.0	Confidentiality	

Contents

Copyright

Disclaimer

QI-ANXIN Group is a network security company focusing on providing enterprise level network security technology, products and services for government, army, enterprise, education, finance and other institutions and organizations, including but not limited to the following subjects: Beijing QI-ANXIN Technology Co., Ltd., LegendSec Information Technology(Beijing) Co., Ltd., Beijing WangKang Technology Co., Ltd, and the legal entities directly or indirectly controlled by the above subjects.QI-ANXIN Group hereby specifically states that it does not assume any legal liability for the following matters:

This product has been tested in detail, but it can not be guaranteed that it is fully compatible with all software and hardware systems or products, and there is no guarantee that this product is completedly error free. In case of incompatibility or error, users can call the technical support telephone to report the situation to QI-ANXIN Group for technical support.

To the maximum extent permitted by applicable laws, QI-ANXIN Group will not be liable for any damages and risks arising from the use or inability to use the product, including but not limited to direct or indirect personal damage, loss of commercial profits, trade interruption, loss of business information or any other economic losses.

For the loss caused by telecommunication system or internet network failure, computer failure or virus, information damage or loss, computer system problem or any other force majeure reasons, QI-ANXIN Group will not take any responsibility, but will try our best to reduce the loss and impact caused to users.

If the user violates the provisions of this Agreement and causes damage to QI-ANXIN Group, QI-ANXIN Group have the right to take measures including but not limited to interruption of use license, stop providing services, restriction of use and legal investigation.

For the product downloaded from the designated site of non QI-ANXIN Group and the product obtained from the media issued by non QI-ANXIN Group, QI-ANXIN Group can not guarantee whether the product is infected with computer virus, whether there is camouflaged Trojan horse program or hacker software. The use of such software may lead to unpredictable risks, It is suggested that users should not download, install and use them, and QI-ANXIN Group will not bear any legal liability arising therefrom.

Any loss or damage (including direct, indirect, special or consequential loss or damage, such as loss of income or profit), caused by the use of the information on the product or the information linked by the product, or other website information linked to the product, for any reason (including but not limited to negligence), in case of damage to computer system or loss of data, QI-ANXIN Group shall not be liable for any legal liability arising therefrom.

The right of final interpretation of the above statement belongs to QI-ANXIN Group.

1 Manual Overview

1.1 Manual Overview

This manual is the "Legendsec Next-generation Firewall White Paper", mainly introducing the background of the emergence of the QAX Firewall, the problems it solves, product features, technical advantages and application scenarios.

1.2 Revision Record

The revision history accumulates descriptions of each update to the document. The latest version of the document incorporates all previous version.

The update contents of the version. Document Version V1.0. The first official release.

1.3 Symbol Conventions

Sign	Illustration
Warning	Indicates a potential hazard which, if not avoided, may result in personal injury.
Caution	Indicates potential risks. If ignored, it may lead to equipment damage, data loss, equipment performance degradation or unpredictable results.
Note	Indicates the additional information of the text, which emphasizes and supplements the text.
Tip	Indicates it can help you solve a problem or save you time.

2 Product Overview

With the rapid development of information technology, the network situation is undergoing rapid and continuous changes, and a constant stream of new threats are challenging the existing security protection system. Traditional security devices have the following problems:

- With the local rule base as the core, it is unable to effectively detect known threats.
- We are at a loss as to how to deal with the various security issues of increasingly rich Web applications.
- Without data intelligence, it is impossible to perceive unknown threats.
- Without intelligent linkage, it is impossible to carry out coordinated defense on the network. In the face of increasingly diverse and hierarchical attacks such as 0-day, APT and unknown threats, it is gradually becoming inadequate.

Ultimately, the traditional security and product systems are still addressing networked and public known threats with the mindset of isolated and private machines. However, when it comes to unknown security threats, we can no longer fight alone. Instead, we must collaborate and share.

Legendsec Next-generation Firewall (hereinafter referred to as firewall) is an independent creation of QAX Group which is new generation firewall security system, based on NDR (Network-based detection and response) security system. Under the support of high performance and advanced architecture, it integrates firewall, WAF, VPN, application and identity, antivirus, intrusion prevention, virtual system, behavior management, application layer content security protection, threat situation report and other comprehensive security defense functions, and support with Skyee, terminal management system, NGSOC, security cloud, etc. Multiple systems perform cooperative defense.

Based on the expanded collaborative defense capabilities, the firewall, with the analysis center, data center and response center as the core, has realized an integrated process of threat analysis, location and response. It is a new generation of network security defense system based on the collaborative defense system, specially designed for the network exits of governments, military, finance, education, operators and enterprises.

3 Product Features

3.1 Flexible management interface

The firewall supports device management through business interfaces or MGT management interfaces, which is suitable for different user environments.

Management Methods	Description
Business Interface	There is no need to build an additional management network, reducing complexity and maintenance. The branch supports management modes via configuration interfaces (HTTPS, Ping, SSH, SNMP) and trusted manager machines, minimizing the management risk.
MGT Interface	The separation of the management plane and the service plane does not affect fire prevention with large amounts of service data. The independent management interface restricts firewall terminals strictly, ensuring firewall management security. Supported management modes under the configuration interface include HTTPS, Ping, SSH, and SNMP, as well as trusted manager machines, minimizing management risks.

3.2 Administrator rights are separated and divided

The firewall supports a role-based, decentralized administrator account mechanism based on administrators, and according to the operational scenario requirements of users:

- The system predefines super administrators, configuration administrators, account administrators, audit administrators, RESTful API administrators, and OpenC2 linkage administrators. While achieving the separation of configuration management, security management, audit management, RESTful API, and linkage functions, it also ensures the isolation of administrator permissions.
- The firewall supports custom administrator roles, and each role can precisely specify the read and write permissions for system functional modules, facilitating user management of the system.

3.3 Virtual system for secure isolation

3.3.1 Overview

The firewall supports the virtual system function, which can virtualize the firewall into multiple isolated and independently operating virtual firewalls, and also supports the division of system resources. Each virtual system can provide customized security protection functions for users and can be equipped with an independent administrator account.

As the user's network expands continuously, the virtual system function can not only effectively reduce the complexity of the user's network but also enhance its flexibility. When these isolated and independently operating virtual firewall systems need to communicate, it can be achieved through the virtual interfaces provided by the firewall, without the need to connect them via physical link.

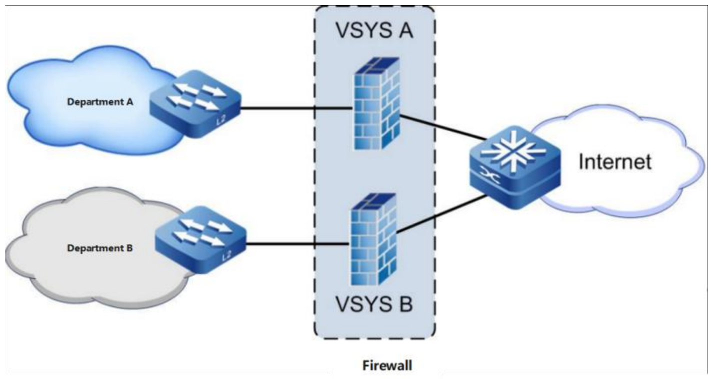


Figure 3-1 Networking Deployment of Virtual Firewall

3.3.2 Multi-function in one device, saving investment

In traditional firewall deployment schemes, the ratio of business servers to firewalls is basically 1:1. Therefore, when business expands, users need to purchase new firewalls. However, when business shrinks, the corresponding firewalls become idle, resulting in wasted investment.

Virtual firewall technology, with its flexible and scalable features, helps users protect their investments. Users can add or remove corresponding virtual firewalls at any time according to the increase or decrease of their business.

3.3.3 Flexible configuration and convenient management

Virtual firewall technology enables data centers to tailor virtual firewalls with different performance metrics based on the performance requirements of customers. For instance, a virtual firewall with a throughput of 10M can be rented to some customers, while a virtual firewall with a throughput of 100M can be rented to others.

3.3.4 Business isolation, no mutual influence

There are various types of business operations, and the firewall security policies required for each are different. For instance, DNS servers need protection against DNS Query Flood attacks, while HTTP servers require protection against HTTP Get Flood attacks. The division of virtual firewalls enables the configuration of exclusive protection policies for different business operations

Meanwhile, CPU resource virtualization supports isolating faults and performance bottlenecks between virtual firewalls. When a single virtual firewall is under attack or runs out of resources, the others will not be affected, greatly enhancing the overall availability of various services

3.4 IPv6 Ready

3.4.1 IPv4/IPv6 Dual Stack

The firewall supports a complete dual-stack protocol and multiple functions under IPv6, including network and security functions. From the user's perspective, it is like supporting two concurrent networks.

Function Items	Description
IPv6 Interface	- Supports IPv6 address configuration on interfaces - Supports device management using IPv6 addresses

	- Supports manual and automatic IP/MAC detection and binding for IPv6- Supports SLAAC functionality - Supports RA (Router Advertisement) issuance
IPv6 Routing	- Supports static routing, policy - based routing, and dynamic routing (RIPng, OSPFv3, BGP4+, IS - IS) under IPv6 - Supports dynamic management and static configuration of IPv6 neighbors
IPv6 Authentication Management	- Supports local authentication for IPv6- Supports IPv6 Web authentication
IPv6 Log Management	- Supports SYSLOG and SNMP for IPv6
IPv6 VPN	- Supports IPv6 IPSec and IPv6 GRE- Supports IPv6 tunneling technologies (6to4, ISATAP, manual tunneling) - Supports DS - Lite functionality, and supports B4 and AFTR networking roles
DHCPv6	- Supports DHCPv6 Server- Supports DHCPv6 Relay
IPv6 DNS	- Supports static DNS - Supports selection of DNS proxy servers based on interfaces, source addresses, or destination address.
IPv6 VXLAN	- Supports serving as a Layer 2 VXLAN gateway, Layer 3 VXLAN gateway, and simultaneously as both Layer 2 and Layer 3 VXLAN gateways
NAT	- Supports NAT - PT, and supports SNAT and DNAT for 4to6 and 6to4 - Supports NAT64 and DNS64 - Supports NAT66, and supports one - to - one, many - to - one, many - to - many, and NPTv6 (ALG only supports FTP and TFTP)
IPv6 Security Features	- Security features based on IPv6 such as leak protection, anti - spyware, URL filtering, anti - virus, content filtering, file filtering, email filtering, behavior control, Web attack protection, etc. - Supports IPv6 extension header security detection and MAC consistency checking

Thanks to the support of the fully independently developed AMP+ architecture and the fourth-generation SecOS operating system, the firewall system can achieve IPv6 performance comparable to that of IPv4.

3.4.2 Cross-stack tunneling solution

The firewall supports multiple cross-stack tunneling solutions, facilitating users' cross-stack message transmission requirements during the IPv6 evolution process. Mainly including:

- 6in4 Cross-stack Tunneling Solution
- GRE Cross-Stack Tunneling Solution
- NAT64/DNS64 solution

3.4.2.1 6in4 Cross-stack Tunneling Solution

The firewall supports 6in4 cross-stack tunnels. It allows IPv6 hosts to access another IPv6 host or IPv6 service through an IPv4 network.

The firewall supports three types of 6in4 tunnels, namely manual tunnels, ISATAP, and 6to4 tunnel

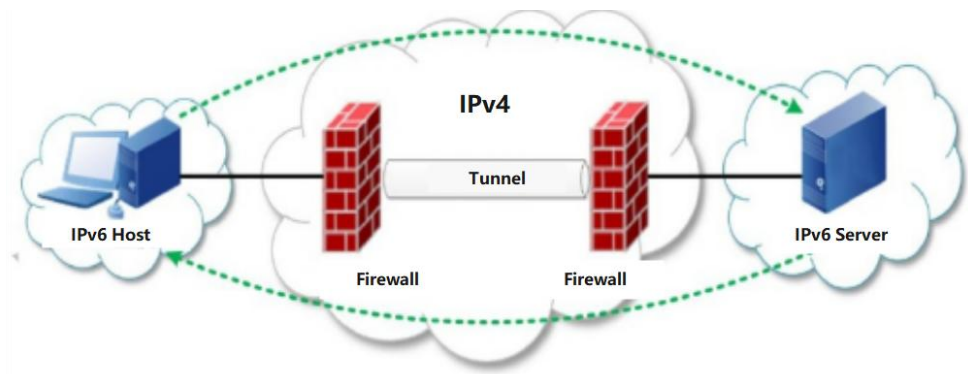


Figure 3-2 Examples of Typical Application Scenarios for Manual Tunnels

3.4.2.2 GRE Cross-Stack Tunneling Solution

GRE （Generic Routing Encapsulation） provides a mechanism for encapsulating the packets of one protocol within those of another, enabling IPv6 packets to be tunneled. Transmit over IPv4 networks.

GRE tunnels can carry IPv6 packets as payloads. By adding GRE headers and IPv4 headers externally, they can be transmitted over IPv4 networks.

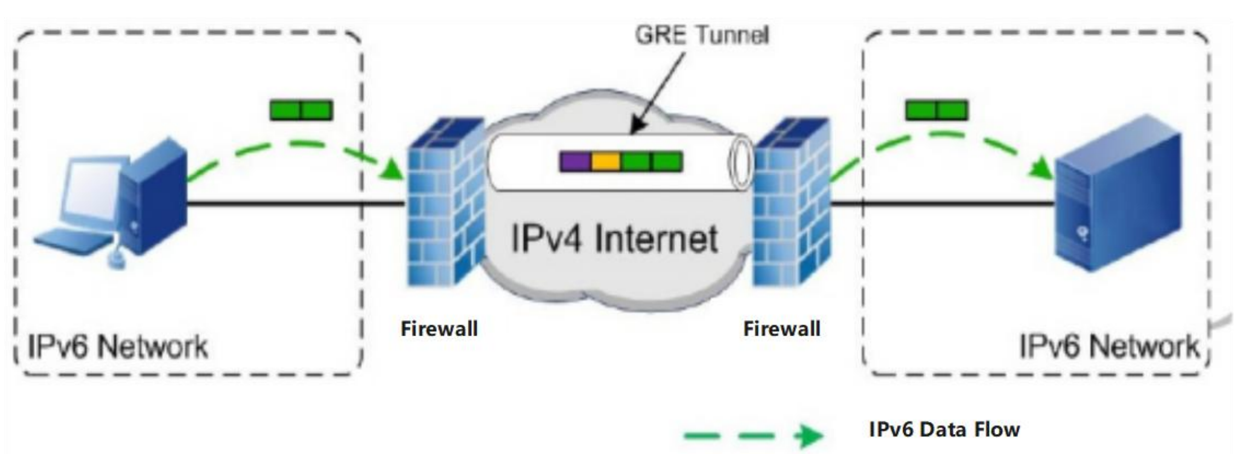


Figure 3-3 Typical Application Scenario of GRE Cross-Stack Tunnel

3.4.2.3 NAT64/DNS64 Solution

During the evolution of IPv6, the readiness of IPv6 on the network side is relatively high, but the IPv6 adoption on the service side is still not optimistic, with a significant portion of resources still using IPv4 addresses. The NAT64 technology is specifically designed to address the issue of address conversion from IPv6 to IPv4 when IPv6 terminals access IPv4 resources.

As shown in Figure 3-4, after applying the NAT64 function on the firewall, the different situations when IPv6 users access the Internet are as follows:

If the destination IP address is an IPv6 address, the firewall will directly forward the message to the corresponding IPv6 network.

If the destination IP address is an IPv4 address, the firewall will convert the IPv6 address in the message to an IPv4 address and then forward it to the corresponding IPv4 network.

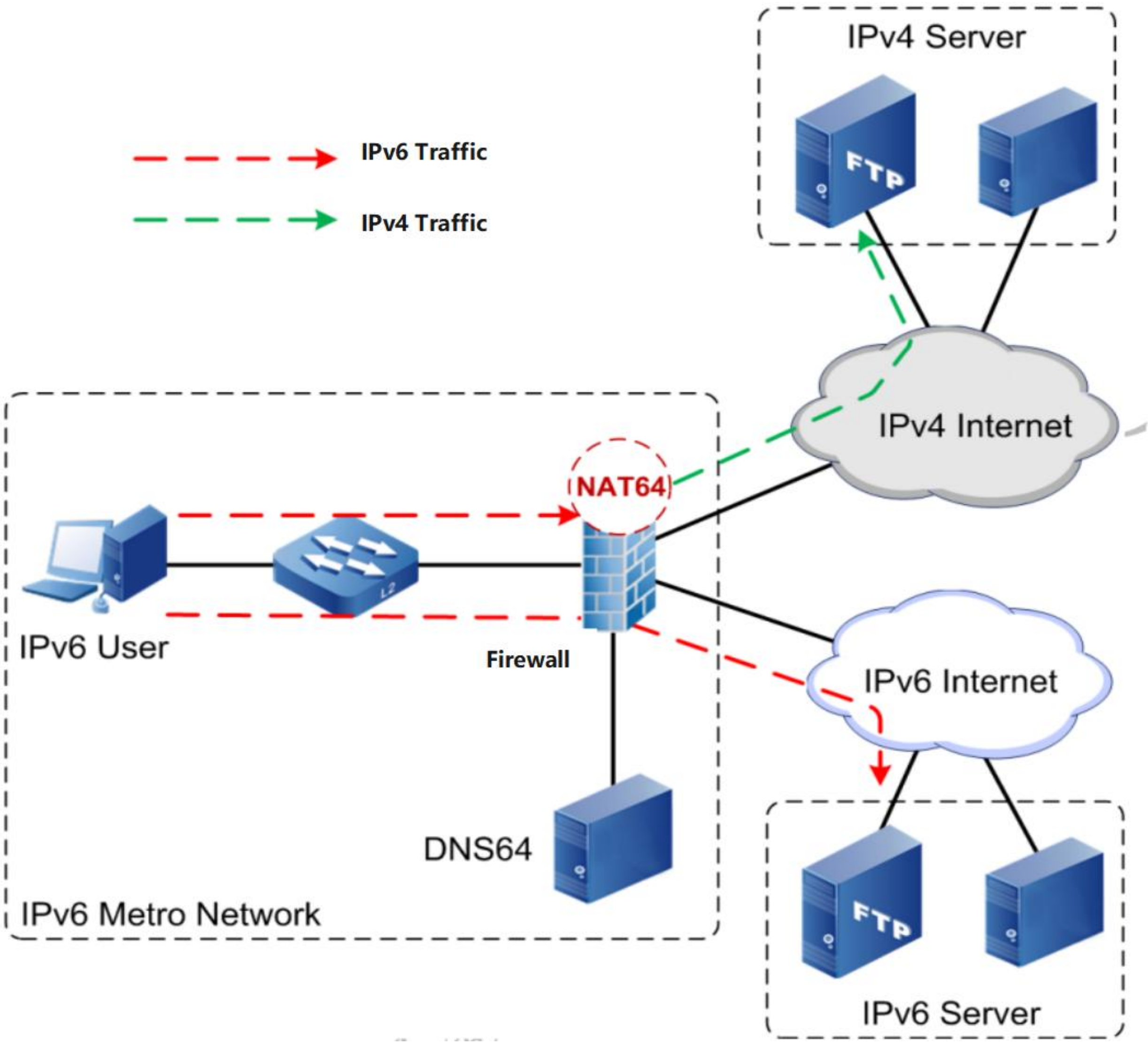
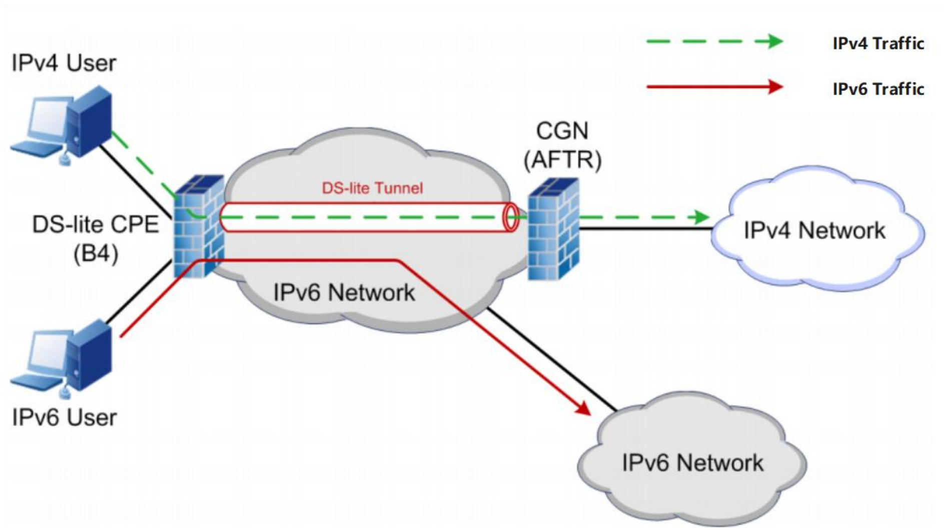


Figure 3-4 Schematic Diagram of NAT64 Application Networking

3.4.2.4 DS-Lite Solution

The firewall supports the DS-Lite lightweight cross-stack tunneling solution and is capable of playing the roles of both B4 and AFTR in the network.

By carrying IPv4 traffic through tunnels in an IPv6 network, the end terminals at both ends of the IPv6 network do not need to support the IPv4/IPv6 dual-stack protocol, ensuring its "lightweight" nature. A typical network configuration is shown in Figure 3-5.



3.5 Multi-level reliability, high reliability of the device

3.5.1 Hardware device reliability

3.5.1.1 Dual redundant power supply

Some firewall models support redundant power supplies and hot-swappable power modules.

- When two power modules are used simultaneously, they share the load.
- If one module fails or is disconnected, the other can fully support the system’s operation.
- The power modules also support hot swapping, allowing users to replace a faulty module without shutting down the system.

3.5.1.2 MGT interface

The firewall supports management via the MGT interface, separating management data from business data. Using the MGT interface provides a more reliable management link than the business interface, ensuring device management and fault location even during high traffic or device failure.

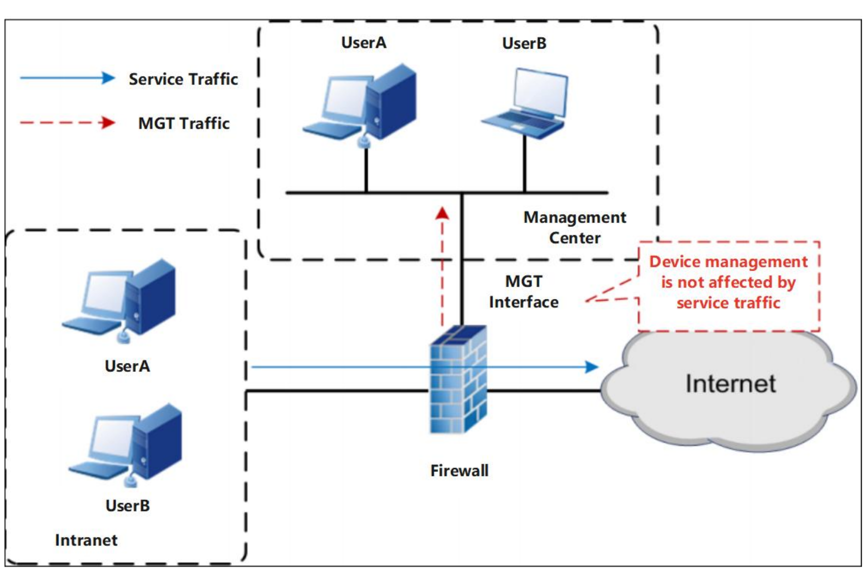


Figure3-6 Out-of-band management

3.5.1.3 Bypass and Watchdog

The firewall supports hardware Bypass and watchdog functions to prevent network failure due to system failure

Hardware Bypass: When the device fails unexpectedly, business flow can bypass the firewall directly, preventing network paralysis caused by a single firewall failure.

Watchdog:When the device system fails, the hardware watchdog automatically reboots it, preventing network paralysis outside the firewall.

Note

The firewall hardware bypass function is implemented by the hardware interface board.

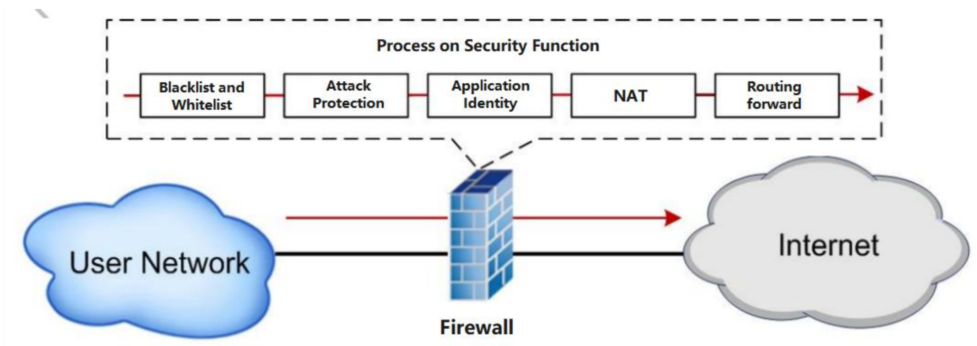


Figure 3-7 Hardware Bypass Principle -- Normal State

3.5.1.4 ECC Storage

Firewall models in the mid-to-high-end range use memory with ECC technology. This ensures long-term system stability by detecting and correcting errors, preventing interruptions and maintaining normal operation.

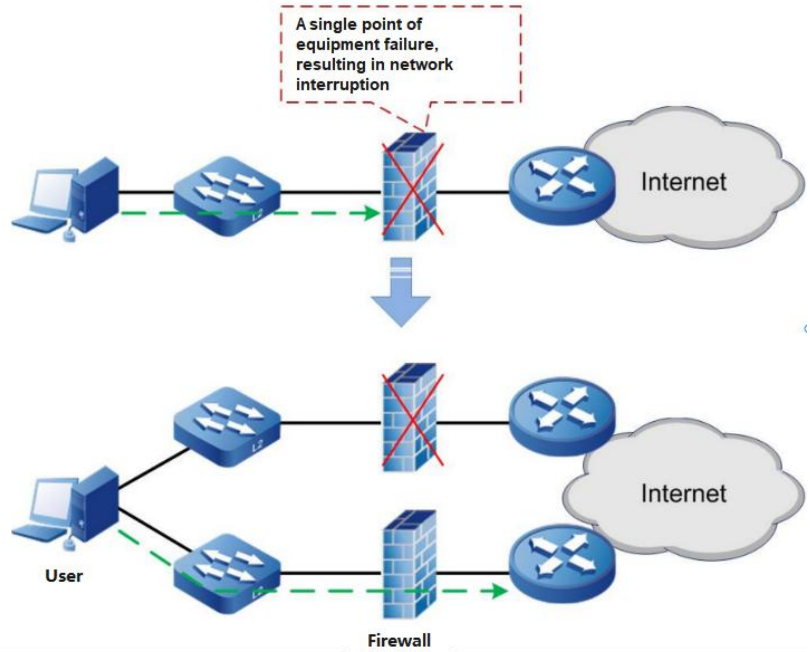
ECC (Error Checking and Correcting) is a technology that detects and corrects errors in memory. It allows systems to continue operating normally without interruption, ensuring stable performance.

3.5.2 Overall machine reliability

3.5.2.1 Overview

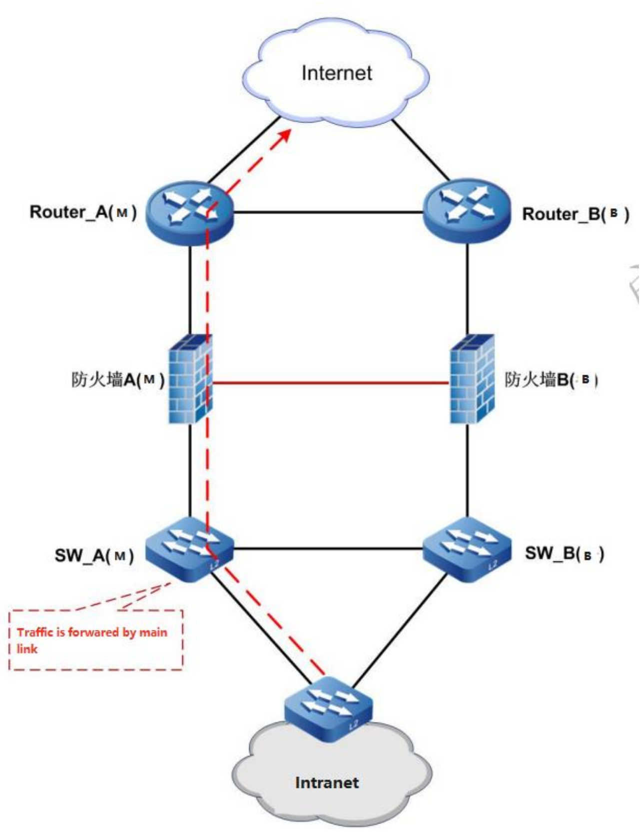
When a single firewall is deployed at the user network's exit point, if the device malfunctions, it will cause a link interruption, which in turn leads to the disruption of the entire business operation.

By deploying dual-server hot standby, two firewalls are placed at critical network positions to enhance network reliability. When one device fails, communication can be maintained through the other device, ensuring the normal operation of business.

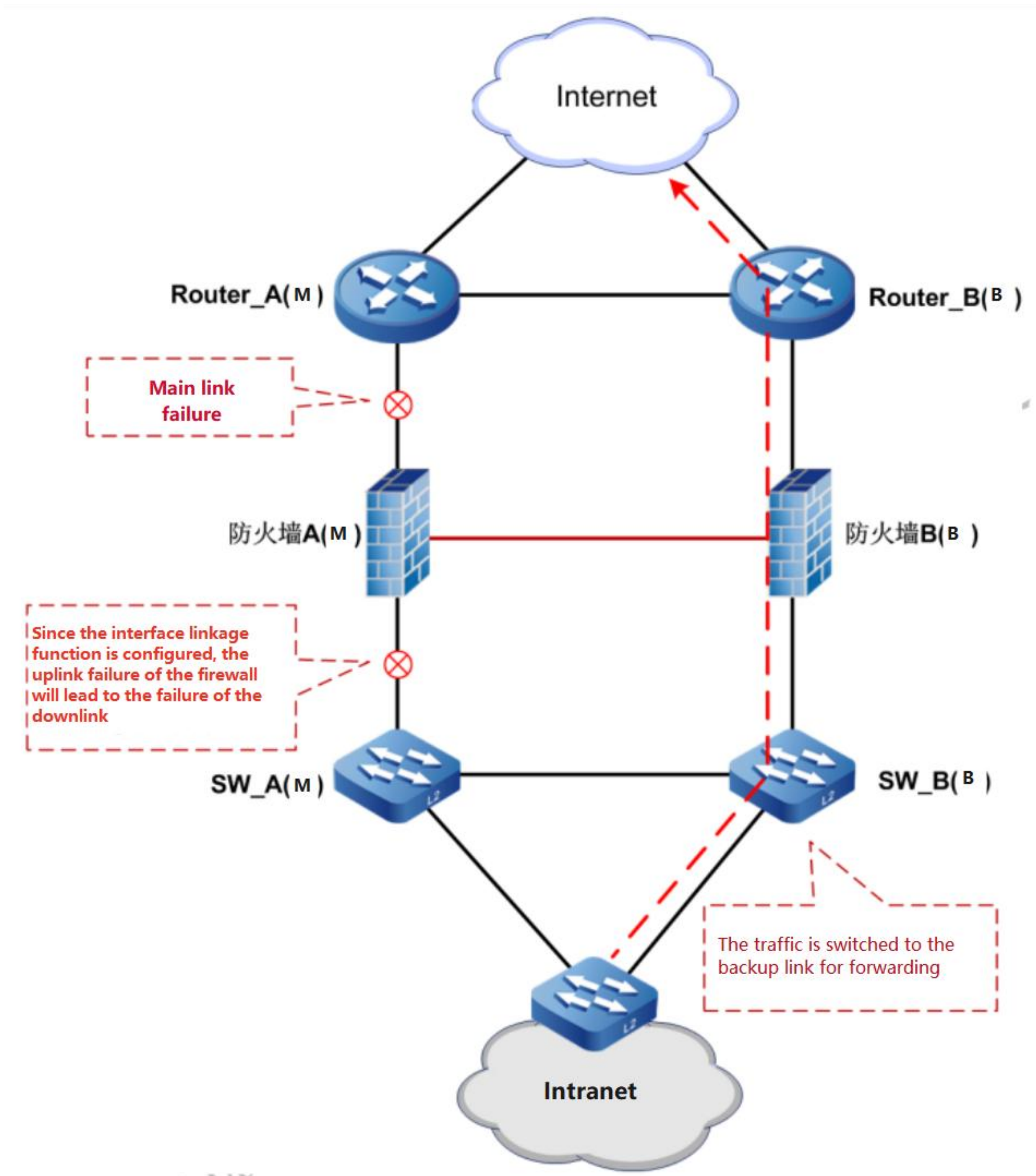


3.5.2.2 Hot-Standby Mode

In the active and standby mode, one of the two firewalls acts as the primary device and the other as the backup device.The primary device is responsible for all the packet forwarding work, and the current session information and configuration information are synchronized to the standby device.



When the primary device fails, it automatically switches to become the backup device, while the original backup device becomes the primary device, takes over packet forwarding, and ensures seamless network handover.



3.5.2.3 Active-Active Mode

In active-active mode, Configure two HA groups on Firewall.

- In the HA group 0, Firewall A is the primary device and Firewall B is the backup device. Under normal circumstances, the traffic of User A is forwarded by Firewall A.
- In HA Group 1: Firewall B is the primary device and Firewall A is the backup device. Under normal circumstances, the traffic of User B is forwarded by Firewall B.

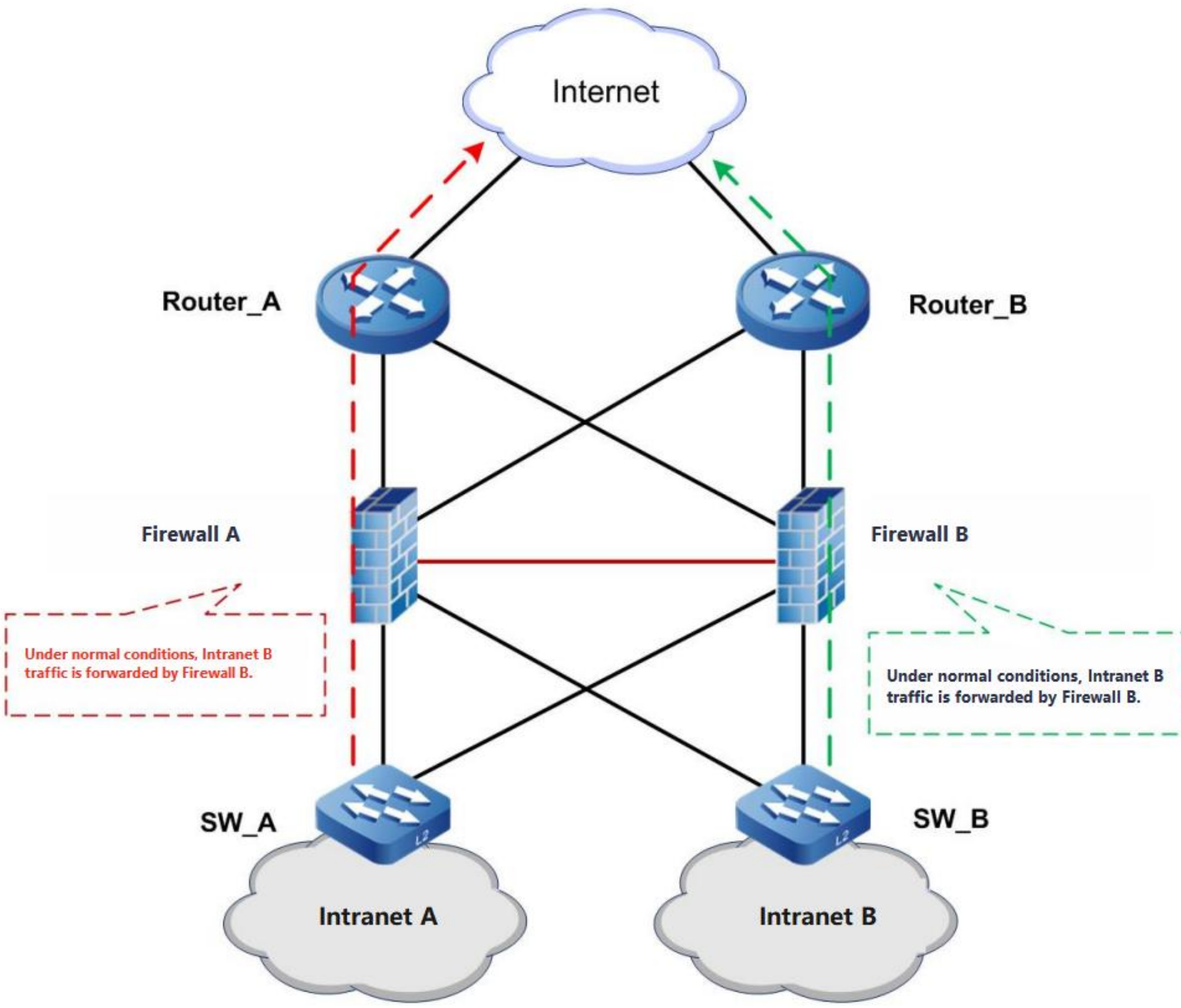


Figure 3-12 Load Balancing Dual-Host Active&Standby (Normal Forwarding State)

When one of the devices malfunctions, the traffic of both HA groups will be switched to the same device for message forwarding.

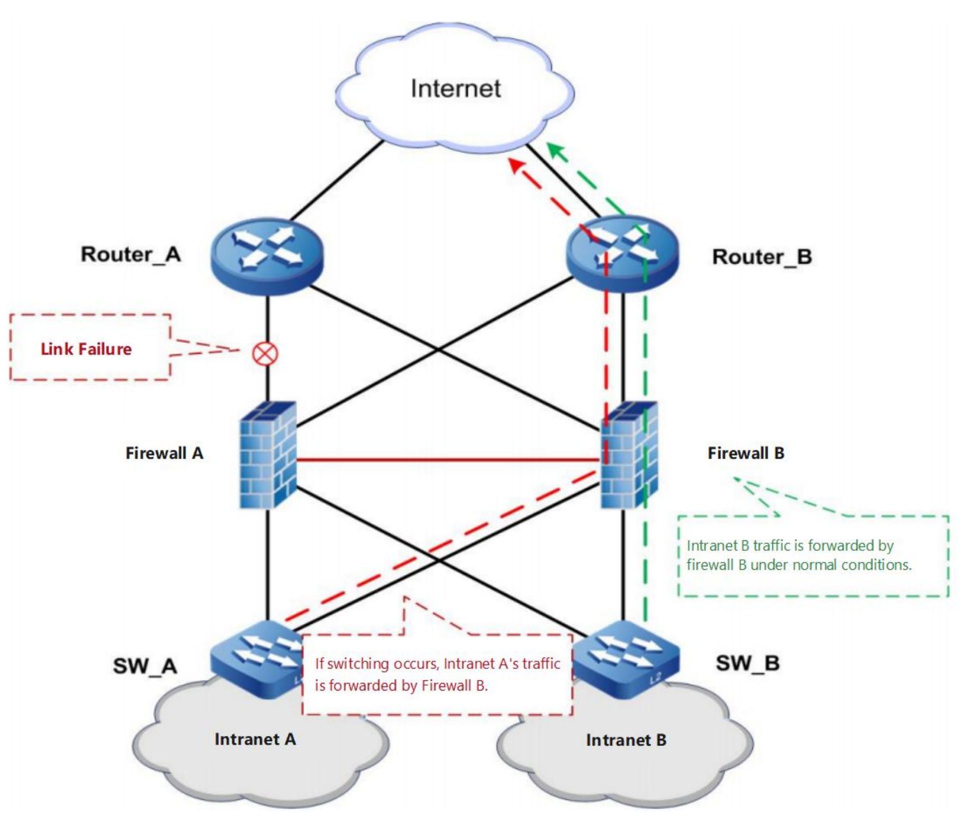


Figure 3-13 Load Balancing Dual-Host Hot Standby (Link Switching State)

3.5.2.4 Dual-server with hot-standby mode for full redundancy networking

Connect SW_A to SW_B as shown in Figure 3.13. Router_A and Router_B are connected, forming a fully redundant dual hot-standby network (see Figure 3-14).

This improves network reliability and prevents business interruptions caused by multiple link failures. For example, if GE1 and GE2 on firewall A and GE1 on firewall B fail, traffic can still be forwarded through GE2 on firewall B.

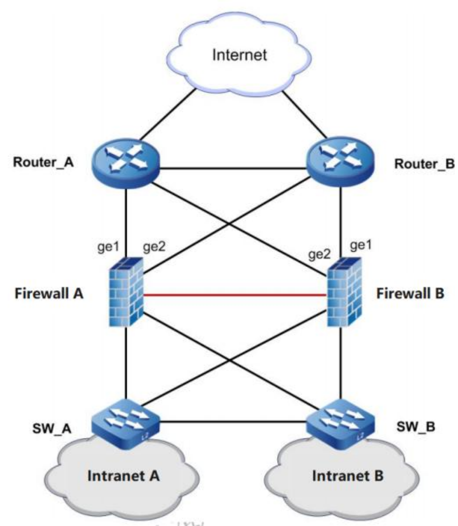


Figure 3-14 Dual-Computer Hot Standby Full Redundancy Networking

3.5.2.5 Information Synchronization

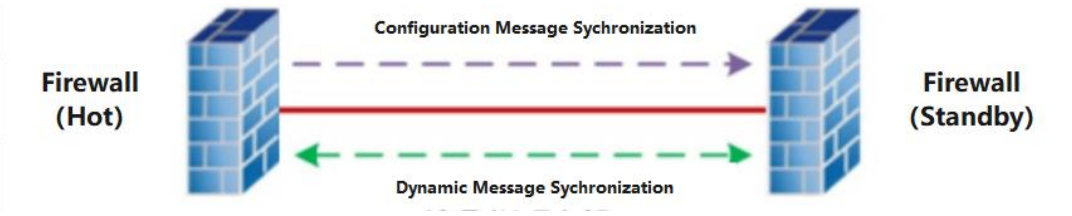
If it is traditional network equipment (such as routers and Layer 3 switches), only the backup of routes on two devices is needed to ensure the reliability of services. That is, when one device fails, the other device can take over the faulty device to handle services and ensure that services are not interrupted.

A firewall, as a stateful inspection device, conducts a complete inspection on the first packet (the first message) of a traffic flow and establishes a session to record the state information of the message (including the source IP, source port, destination IP, destination port, protocol, etc.). Subsequent messages of this traffic flow can only pass through the firewall and be forwarded if they match the session.Otherwise, they will be discarded by the firewall. Therefore, when deploying dual firewalls, it is also necessary to consider the backup of session and other state information between the two firewalls.

- Configuration information synchronization: Once the primary wall completes configuration and enables the HA function, the configuration information will be automatically synchronized to the secondary wall, ensuring that the secondary wall has exactly the same configuration as the primary wall. The configuration information is unidirectional synchronized from the primary wall to the secondary wall.

- Dynamic information is generated during data forwarding by the firewall, such as session information and timeout periods. The hot and standby firewalls can synchronize this type of information in real time to ensure consistency.

The dynamic information of the primary wall and the backup wall is consistent. The dynamic information is bidirectional, allowing the primary wall and the backup wall to synchronize with each other.



3.5.3 System reliability

The firewall supports dual-system backup:

- When the main system malfunctions, it can be switched to the backup system to continue providing services.
- When the system upgrade fails, the backup system can be used to start the firewall to achieve a rollback of the upgrade.

3.5.4 Link reliability

3.5.4.1 Link Aggregation

Manual static link aggregation.

The firewall supports manual static link aggregation. The manual aggregation method combines multiple physical ports into a Trunk group to form a logical port. The links under the same logical port achieve load sharing. However, this approach is not conducive to observing the status of the link aggregation port.

802.3ad Link Aggregation Method

The link aggregation method that complies with the IEEE 802.3ad protocol adopts the LACP (Link Aggregation Control Protocol) protocol. The LACP protocol exchanges information with the opposite end through LACPDUs (Link Aggregation Control Protocol Data Units). After enabling the LACP protocol on a certain interface, this interface will notify the opposite end of its system LACP protocol priority, system MAC, port LACP protocol priority, port number and operation key by sending LACPDUs.

After receiving the LACPDU from the opposite end, the information therein is compared with the information received from other interfaces to select the port that can be in the "Selected" state, so that both sides can reach an agreement on which port is in the "Selected" state. The operation key is used during link aggregation, where the aggregation control is based on the port configuration (i.e., speed).

A configuration combination automatically generated based on information such as rate, duplex mode, Up/Down status, and basic configuration. In the aggregation group, ports in the Selected state have the same operation key.

The firewall supports three different traffic load algorithms, as shown in Table 3-1.

Table 3-1 Link Aggregation Traffic Load Algorithm

Load balancing algorithm	Description
According to the IP address and TCP/UDP port combination balance	Using IP address and TCP/UDP port hash algorithm
According to the source and destination MAC address combination balance	Using Source and destination MAC hash algorithm
According to the MAC address and IP address	Using MAC address and IP address hash algorithm

combination balance	

Hot standby mode link aggregation

In the hot standby mode, the interfaces included in the aggregation group are in a hot standby relationship, with one interface being the primary and the rest being the backups. During normal operation, only one interface is responsible for packet transmission and reception. When a fault is detected, it switches to one of the normal backup interfaces. As shown in Figure 3-15.

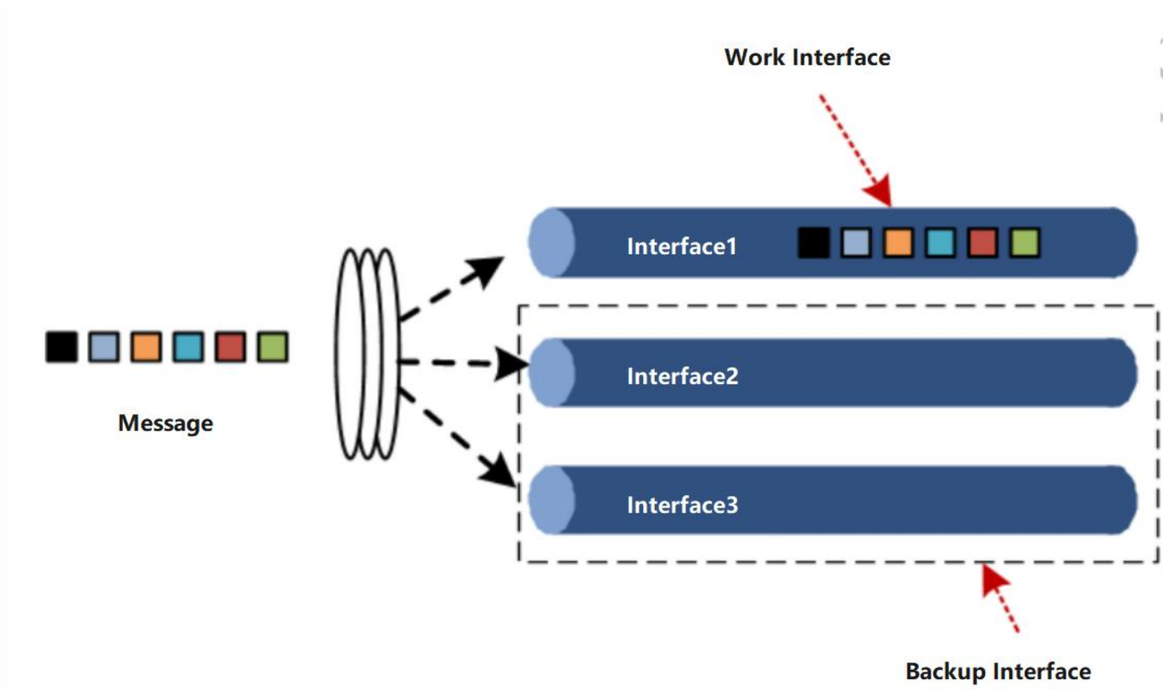


Figure 3-15　Hot Standby Scheduling Mode

3.5.4.2 Interface linkage

Interface linkage solution can expand the scope of link backup. That is, by monitoring the upstream link and synchronously setting the downstream link, faults of the upper-layer devices can be promptly conveyed to the lower-layer ones, thereby triggering link switching and avoiding traffic loss due to the lower-layer devices' inability to perceive faults in the upstream link.

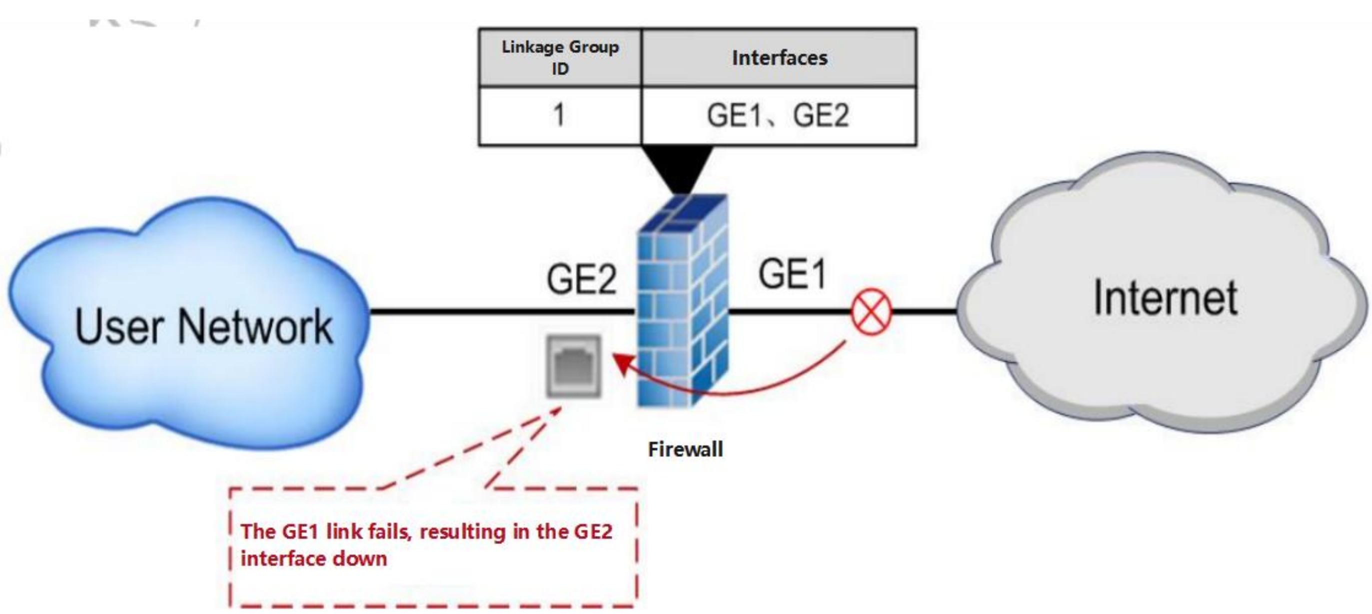
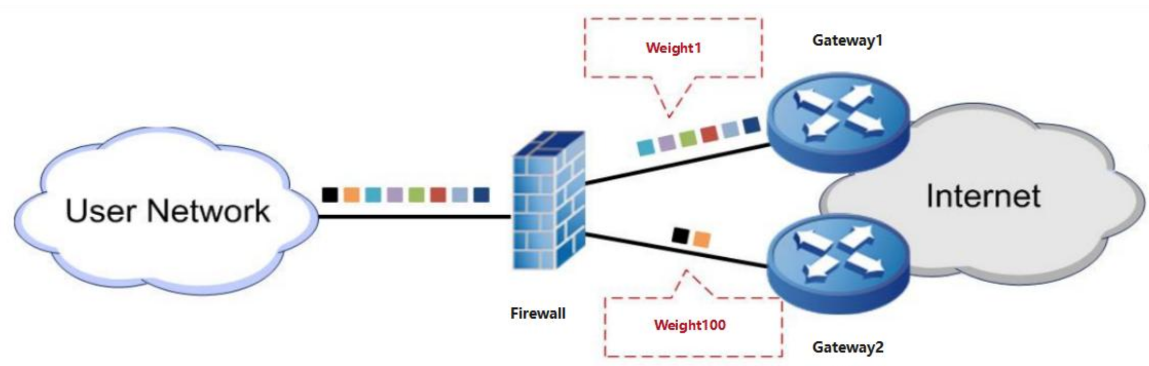


Figure 3-16 Interface Linkage

3.5.4.3 Routing Load Balancing

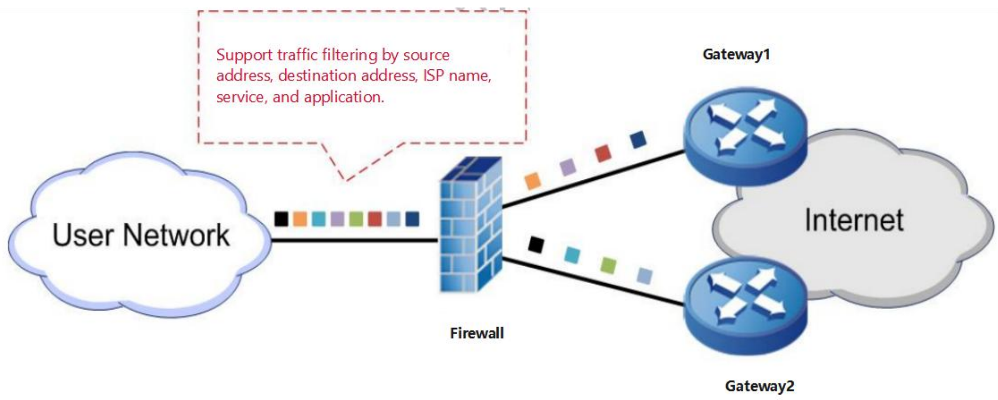
Load balancing based on static routing

The firewall supports traffic load balancing based on multiple static routes. Users can configure multiple gateways according to their actual network setup. The priority among multiple gateways is determined by route weights. When users configure multiple static routes, the higher the weight, the more sessions will be allocated.



Load balancing based on policy-based routing

When a user has two or more exit networks, they can use policy-based routing to filter traffic, achieving the goal of accessing the Internet through different exits based on the characteristics of different traffic flows, and at the same time, link load balancing can be realized.



The firewall can not only divert traffic based on traffic characteristics, but also configure multiple gateways for traffic with the same characteristics and balance the load based on different strategies.

The traffic load balancing methods supported by the firewall's policy-based routing are as shown in Table 3-2, "Policy-based Routing Traffic Load Balancing Methods".

Table 3-2 Load Balancing Methods for Policy-Based Routing Traffic

The firewall supports the ISP information library, which stores destination IP addresses of operators such as China Telecom, China Unicom, China Mobile, and the Education Network. By directly specifying the operator name in the ISP routing, it is possible to access the IP addresses of the corresponding operators through the exit links of different operators.

Meanwhile, for the same ISP operator, multiple gateways can also be configured. The priority among multiple gateways is determined by the routing weight. When users configure multiple static routes, the higher the weight, the more sessions will be allocated.

Load balancing based on ISP routing

The firewall supports an ISP information database that stores destination IP addresses for major carriers. By specifying the carrier name in the ISP route, traffic can be routed to the corresponding operator's IP address through different egress links. Additionally, multiple gateways can be configured for the same ISP, with routing weights determining priority. Higher weights result in more

Load Balancing Methods	Description
Hash based on source and destination address	When the primary device fails, it automatically switches to become the backup device, while the original backup device becomes the primary device, takes over packet forwarding, and ensures seamless network handover.

sessions being assigned.

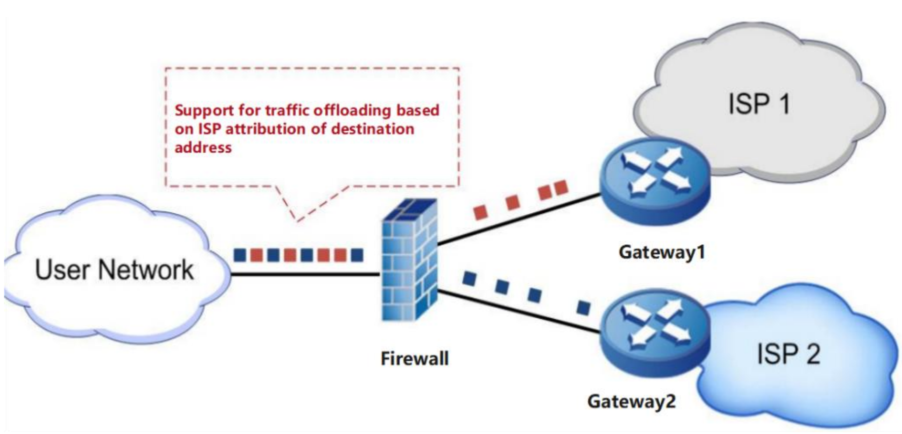


Figure 3-19 ISP Route Load Balancing

3.6 Comprehensive and intelligent routing function

3.6.1 Comprehensive routing functions

The firewall supports comprehensive and complete routing functions. This expands the network adaptability of the firewall system when working in routing mode and its adaptability to IPv6 networks.

Support static routing functions, including IPv4 static routing and IPv6 static routing.

Support static multicast routing and dynamic multicast routing.

It supports multiple dynamic routing protocols, such as RIP, OSPF, BGP, RIPng, OSPFv3, BGP4+ and ISIS.

3.6.2 Precise multi-exit ISP intelligent routing

The ISP routing function mainly provides users with a selection strategy for routing exits based on different operators. It is often used in scenarios where users access the Internet through multiple exits, and each exit corresponds to a different operator.

Often, the speed of accessing services across different operators is slightly slower. Therefore, we hope that if the destination address is to China Telecom, we can add a corresponding static route to the destination address pointing to the China Telecom exit. However, the address range of operators is usually too large. If static routes are added manually, it will be a very troublesome and time-consuming task for users.

The ISP routing intelligent path selection function provides a fast way to add operator routes, and it also supports referencing ISP routes in policy routing. Users can directly select the operator address information preset by the firewall, or write the address range of the operator as a text document and import it into the firewall system. Then, add an ISP route corresponding to each operator's exit.

3.6.3 Symmetric routing ensures that the return path is the same as the outgoing path.

The firewall supports symmetric routing functionality. Users can enable the symmetric routing function of the interface. In this way, users access from where they come in will be returned from the same place. For example, if a user provides an HTTP service on the internal network and has applied for two exits, one from China Unicom and the other from China Telecom, when a user from China Unicom accesses the HTTP service through the China Unicom exit, the symmetric routing function can ensure that the server's response data is also sent back through the China Unicom exit. When a user from China Telecom accesses the HTTP service through the China Telecom exit, the symmetric routing function can ensure that the server's response data is also sent back through the China Telecom exit. This ensures the consistency of the data's round-trip path.

3.6.4 Highly Adaptive Routing Load Balancing Algorithm

The firewall supports matching multiple load balancing algorithms based on users' actual needs in a multi-exit environment, including backup, round-robin, source address hash, source and destination address hash, destination address hash, source address round-robin, optimal link bandwidth load, optimal link bandwidth backup, random, traffic balancing, delay load, hop count load, and so on, totaling twelve types. It can achieve weighted routing load balancing, delay-based routing load balancing, session-based routing load balancing, and traffic-based routing load balancing, meeting various user scenarios.

3.7 Deploy flexible and elastic scalable traffic orchestration

The firewall supports traffic orchestration functions. By reconfiguring the deployment architecture of security devices, pooling security device resources, on-demand traffic diversion based on business needs. it realizes a more flexible deployment method for security devices and a traffic orchestration solution integrating SSL decryption and multiple security capabilities.

The physical connection of security network elements in the traffic orchestration solution has undergone significant changes compared to the traditional deployment method of security devices. Unlike the traditional "beads on a string" approach, in the traffic orchestration solution, both the inline security network elements and the bypass security network elements are directly connected to the traffic orchestration device.

When the traffic passes through the traffic orchestration device, it is diverted to the security network element according to the traffic diversion policy for security processing. After being processed by the security network element, the traffic is forwarded back to the traffic orchestration device, which then receives the traffic.

Then it is forwarded to the next security network element. After all the security network elements have completed processing, it is sent to the original destination of the traffic.

The forwarding path of traffic is determined by the service chain and the traffic diversion policy. The process of defining the service chain is the process of security orchestration of the security network elements in the resource pool. The process of defining the traffic diversion strategy is the process of identifying business traffic. Business traffic can be defined by elements such as five-tuples, security domains, and users. Traffic is diverted to the matching service chain according to the traffic diversion strategy and forwarded according to the logical topology of the serial connection relationship of the service chain.

For a connection, the traffic orchestration device ensures that all security network elements see a consistent five-tuple of the internal network view.

In the traffic orchestration solution, SSL-encrypted traffic only needs to be decrypted once by the firewall. The firewall can then sequentially divert the decrypted plaintext traffic to each network element in the service chain. After the service chain processing is completed, the traffic is sent back to the firewall, which encrypts it and sends it.

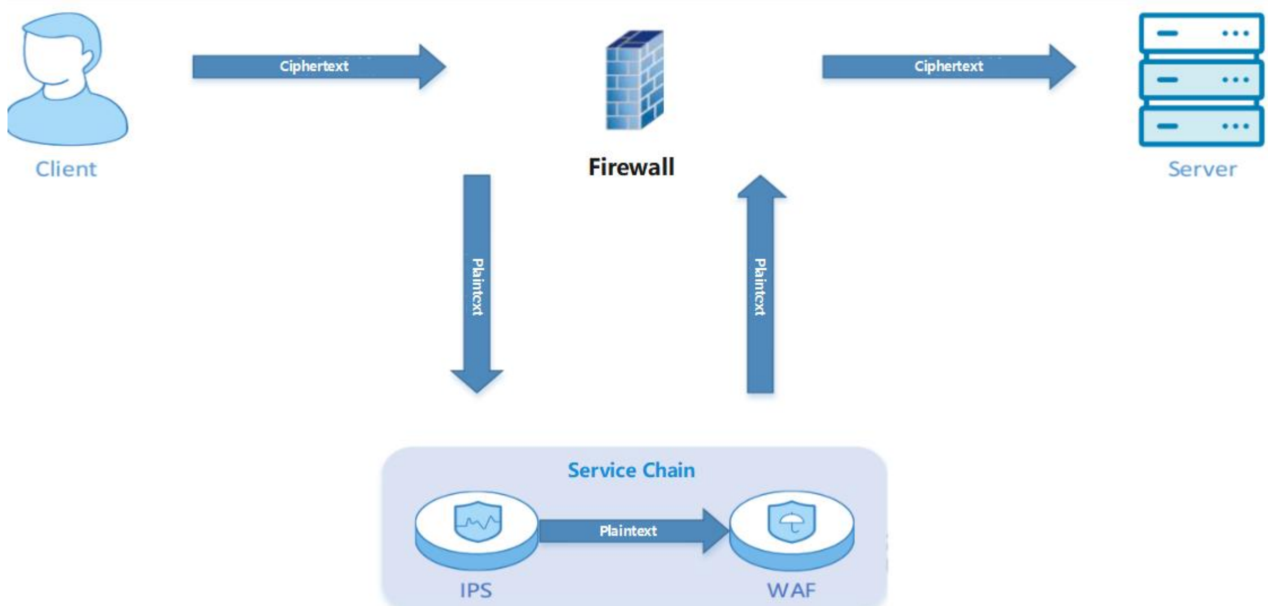
- One traffic decryption can be utilized and processed multiple times by several security network elements.
- Reduce the encryption and decryption resource consumption of security network element

- Provide a deployable environment for secure network elements that do not have encryption and decryption capabilities.
- The security network element can focus on the security processing capability of plaintext.

The traffic is subject to in-depth content security detection and protection (including anti-virus, vulnerability protection, anti-spyware, URL filtering, file filtering, content filtering, email filtering, behavior control, etc.).

For the traffic that passes the content security check and protection, that is, the traffic that does not hit the keywords or the action is not blocking and is not blocked, the firewall will re-encrypt it to ensure that the traffic decrypted by the firewall remains secure when it leaves the firewall.

For traffic that fails the content security check and protection, the firewall will carry out blocking operations, effectively intercepting SSL-based encrypted traffic attacks and information leaks.



3.8 SSL Decryption

SSL is a critical technology for securing transactions on the Internet. HTTP typically transmits data in plaintext, making it vulnerable to eavesdropping. SSL encryption (HTTPS) protects data during transmission by encrypting HTTP traffic. However, this encryption also challenges firewall security detection, as encrypted data cannot be analyzed for threats, viruses, or unauthorized transfers. The SSL decryption function addresses this issue by allowing firewalls to decrypt SSL traffic, perform deep content inspections (e.g., anti-virus, vulnerability protection, URL filtering), and re-encrypt the traffic if it passes checks. If threats are detected, the firewall blocks the traffic, ensuring secure data transmission.

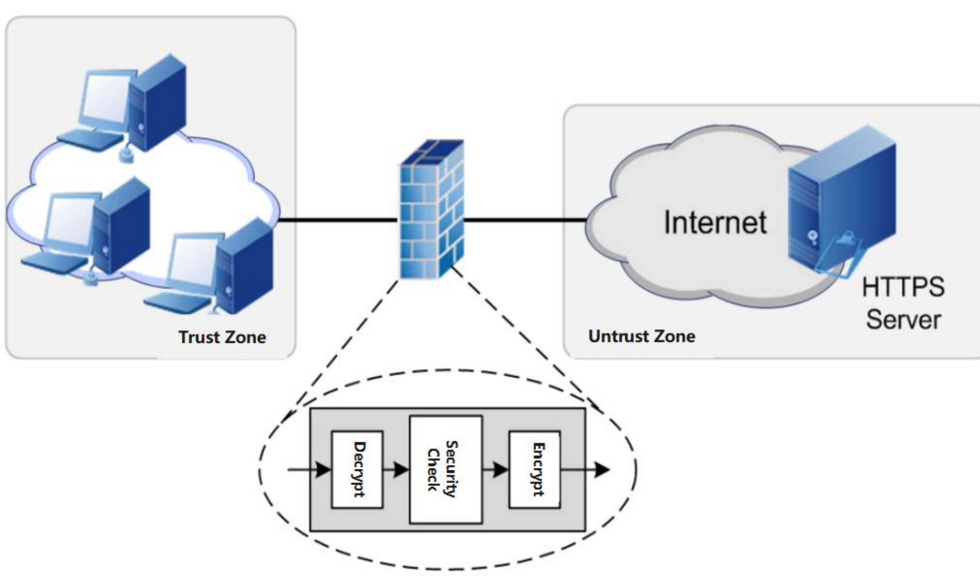


Figure 3-20 SSL Decryption Function

3.9 Multiple VPN tunnels Types

The firewall supports multiple forms of VPN tunnels, fully covering Client-to-Site and Site-to-Site application scenarios. These include: PPTP VPN, L2TP VPN, GRE, IPSec VPN and SSL VPN, and it also supports L2TP over IPSec VPN, GRE over IPSec VPN and DS-Lite.

Meanwhile, the firewall supports multiple types of 6in4 tunnels, including manual tunnels, ISATAP, 6to4 tunnels, and DS-Lite, ensuring access from IPv6 networks to IPv4 networks.

3.10 Powerful recognition function, achieving refined management and control

3.10.1 User Identification

Users are the main body of network usage and the basis for management and control. The core of user-based network behavior management and control lies in the identification and classification of network users.

The firewall supports behavior control policies based on users, which facilitates the administrator's auditing of internal network behaviors in the enterprise. The administrator no longer deals with monotonous IP addresses but specific names of individuals, enabling them to identify violators in the network very intuitively. This enhances network management efficiency and ensures information security.

User identification and control have a natural adaptability to BYOD because no matter what terminal a user uses to access the network or how many IPs the user uses for internet access, they can all be directly mapped to the form of a username, facilitating network administrators' auditing.

As shown in Figure 3-21, network administrators can manage and control online behaviors based on different granularities.

- Control based on "individual users". Administrators can define the Internet access rights and time for each individual user, facilitating more refined permission control within the same user group. For instance, within the R&D department, the manager has the right to access the Internet, while other employees do not.

- Control is based on "user groups". Administrators can map real-world departments to user groups in the system and define the Internet access permissions for each user group. This solution enables batch configuration of user behaviors. When an employee joins or leaves a department, it is only necessary to add or remove them from the user group, simplifying the configuration process.

- Control based on "user roles". Administrators can categorize different users according to roles and define the Internet access permissions for each user role. This solution enables batch configuration of user behaviors. When an employee joins a role, it is only necessary to add or remove them from the role, which is simple and efficient.

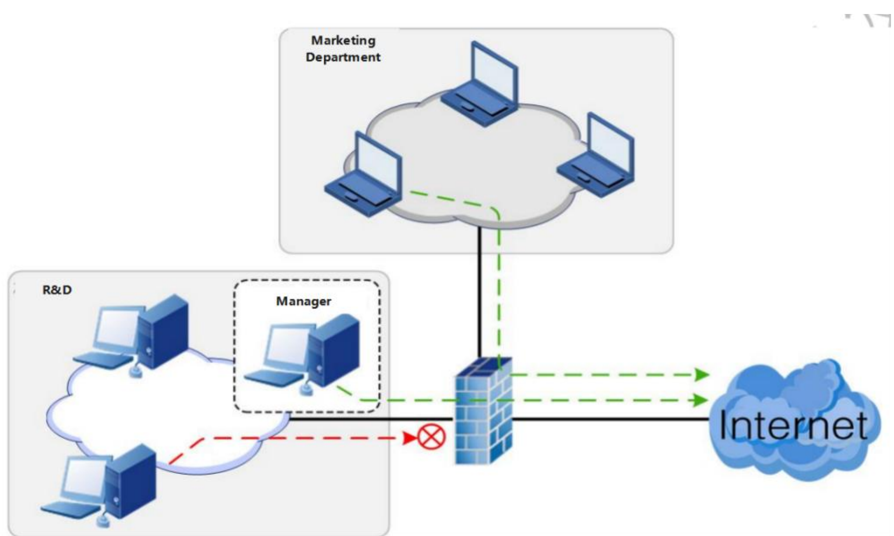


Figure 3-21 User-based Identification and Control

3.10.2 Service Identification

The firewall supports services identification based on TCP and UDP protocols, through source port numbers, destination port numbers and protocol numbers.

The firewall is equipped with a service library of common protocols, allowing users to directly select protocols from the library when in use. It also supports custom services, which are defined by the source and destination port numbers of TCP and UDP protocols.

Default services and custom services can be used as an attribute of security policies to achieve fine-grained traffic control based on services.

As shown in Figure 3-22, an internal network prohibits users from accessing FTP services. This can be achieved by implementing control based on the FTP service (i.e., TCP protocol with destination port 21) on the firewall and configuring relevant security policies.

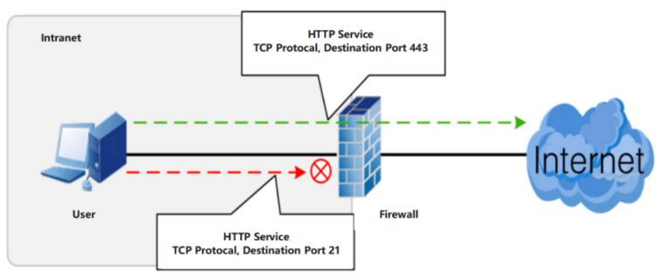


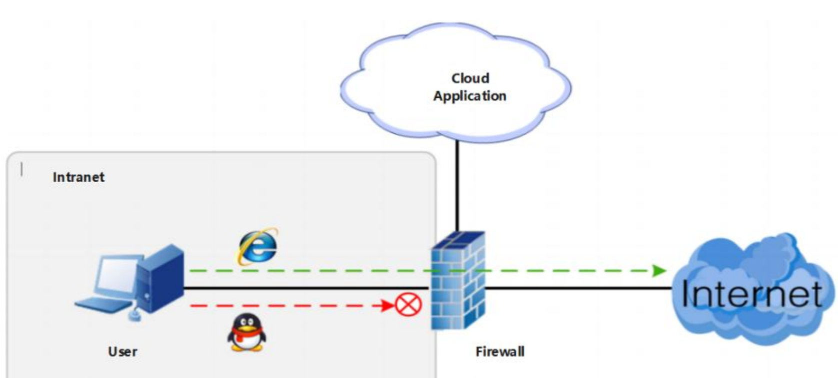
Figure 3-22 Service-based Identification and Control

3.10.3 Application Recognition

The firewall supports an application recognition library, including over 7,000 application features. Through the application recognition library, the firewall can identify applications in the traffic.

Application-based traffic identification and control is used to restrict the use of certain specified applications by users within the network. This method can differentially restrict the use of applications that affect work efficiency or consume a large amount of bandwidth, such as QQ and P2P software, without limiting users' access to the Internet.

As shown in Figure 3-23, an internal network prohibits users from using the QQ software. This can be achieved by implementing behavior control based on the QQ application on the firewall and configuring relevant security policies.



3.10.4 Content Recognition

The firewall supports behavior control policies based on deep content recognition to restrict the dissemination of confidential information within the enterprise network, thereby reducing the risk of company secrets being leaked and ensuring information security.

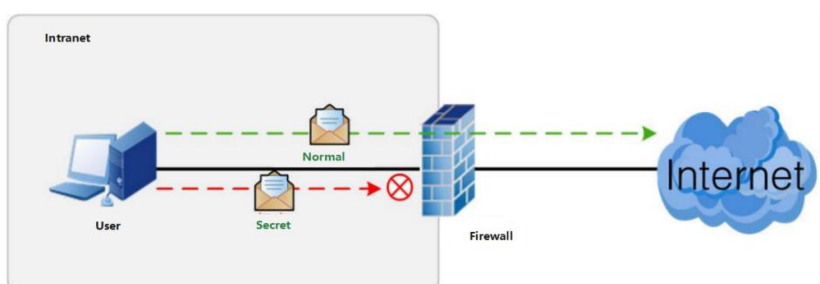
The content recognition function supports both file content recognition and application content recognition.

- File content recognition: It refers to the identification of both the file name and the content of a file. For instance, when a user uploads a Word document, the system recognizes both the document's name and its content.

- Application content recognition: It refers to the recognition of the content of an application. For instance, when a user posts on the Internet, the system recognizes the title and content of the user's post.

As shown in Figure 3-24, when a user attempts to disseminate the company's confidential information to the external network, the firewall, upon receiving the relevant message, scans and identifies the content of the message. If the message contains confidential information fields or fields that do not comply with legal regulations, it will block the message.

Meanwhile, normal messages without corresponding fields are not affected and can be sent and received normally.



3.10.5 URL Recognition

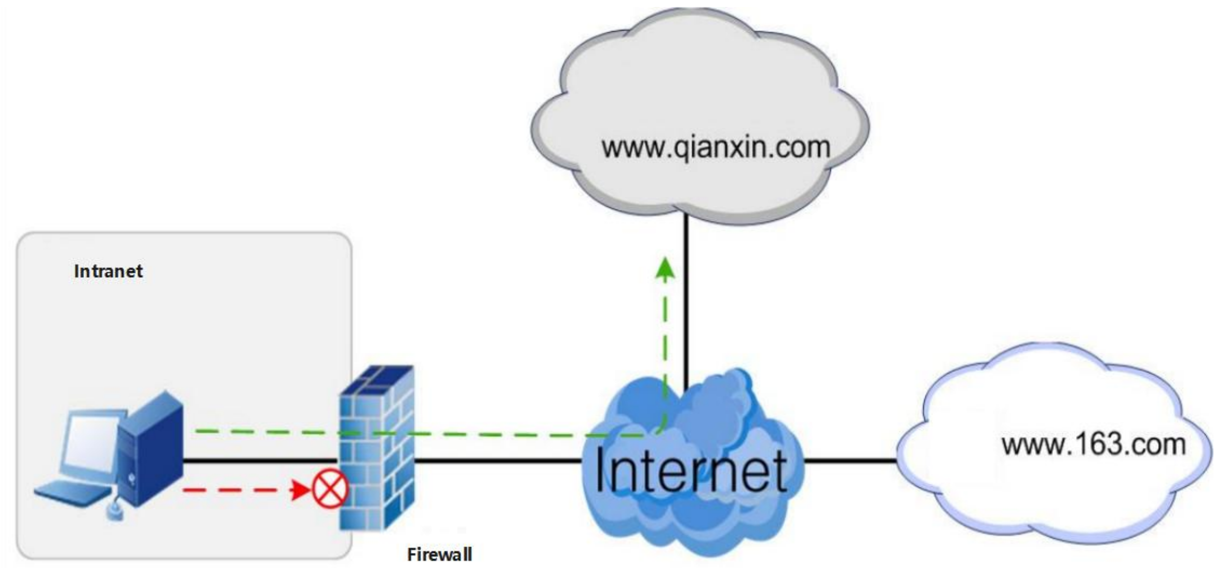
Firewalls support URL-based identification and control, which can be used to restrict internal network users from accessing certain special URLs. This can help improve work efficiency and reduce legal risks. For example, it can prohibit access to pornographic or subversive URLs.

The firewall supports custom URLs. The system detects the URL field in the HTTP request header and allows or denies the request based on the configured control policies.

- For allowed requests, users can directly access the site.
- For prohibited requests, send a message to the user indicating that access is denied.

In addition, the system's built-in URL classification library can be used to deny users' access to certain types of websites.

As shown in Figure 3-25, a certain internal network prohibits users from accessing www.163.com. This can be achieved by implementing behavior control based on URL on the firewall and configuring relevant security policies.



3.10.6 Behavior Recognition

The application behavior control function of the firewall supports precise control over users' HTTP behavior, FTP behavior, SMTP behavior, POP3 behavior, IMAP behavior and Telnet behavior.

In enterprises, it is usually necessary to manage the behavior of internal network users. Different users need different permissions to access network resources through different protocols, and the same user often has different permissions at different times. The application behavior control of firewalls can well meet the above requirements.

As shown in Figure 0, the firewall is deployed at the exit as the enterprise's exit gateway. By configuring the application behavior control function on the firewall, when internal network users access the external network, the behavior of internal network users can be effectively managed.

Multiple application behavior control configuration files can be created on the firewall, each of which is used to control users with different permissions. Then, by referring to the application behavior control configuration files, users and time periods (working hours, non-working hours) and other objects in the security policy, the purpose of differentiated and refined management of the behavior of internal network users can be achieved.

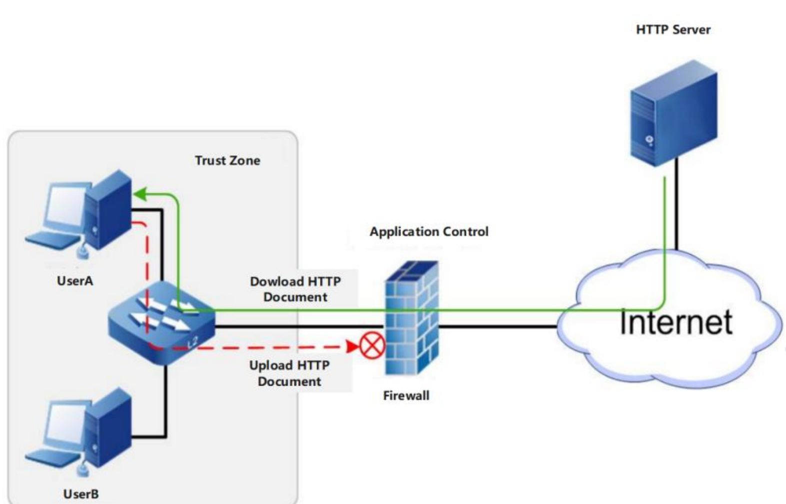


Figure 3-26 Identification and Control of Application Behaviors

3.10.7 Geographic location identification

The firewall supports the geographical location identification function, capable of identifying domestic and international IP addresses, and mapping IP addresses to specific locations.

Users can use geographical location as an attribute to configure security policies. By identifying users through their locations, one can understand the current network usage in different regions, view traffic trends, threat trends, etc. based on geographical locations, and thus adjust firewall policies for different geographical locations, providing a new control perspective for users' security policy management.

3.10.8 Refined security policies

The security policy of a firewall is its core function and the foundation for it to implement access control.

The firewall supports dynamic packet filtering technology based on state detection and application layer data recognition. It identifies data through dimensions such as source security domain, destination security domain, source MAC address, destination MAC address, source IP address, destination IP address, geographical location, user, service, application, and time, separates the data streams that users need to filter and control, and achieves fine-grained management and control.

Meanwhile, the firewall supports the integrated policy configuration for anti-virus, vulnerability protection, anti-spyware, URL filtering, file filtering, content filtering, email filtering and behavior control for the corresponding data

3.11 Deep security detection and DLP, protecting network security

3.11.1 Overview

Firewalls possess the capabilities of in-depth data security inspection and attack defense. They mainly include:

- Attack protection: Supports DoS/DDoS protection, malformed packet protection, DHCP protection, etc.
- Intrusion prevention: Supports vulnerability protection, spyware protection, web protection, virus protection, etc.
- DLP (Data Loss Prevention):It supports email filtering, file filtering, content filtering, etc.
- Unknown threat protection: Supports threat intelligence, 0-day threat protection, APT unknown threat protection, etc.
- Application attack protection: Supports professional web attack protection.
- Vulnerability canning: Supports vulnerability scanning services

3.11.2 Comprehensive application layer attack protection capabilities

The firewall is based on security domains and supports multiple types of attack protection.

- Flood protection: This includes protection against SYN Flood, ICMP Flood, UDP Flood, IP Flood, DNS Flood and HTTP Flood.
- Malicious scanning protection: This includes Tracert scanning, IP address scanning and port scanning.
- Deception protection: This includes IP spoofing and DHCP protection.
- ICMP control. This includes prohibiting ICMP fragmentation, prohibiting route redirect messages, prohibiting unreachable messages, prohibiting time-exceeded messages, and setting size limits for ICMP messages.
- ICMPv6 control. This includes disabling unreachable messages, disabling packets too big messages, disabling time exceeded messages, disabling parameter problem messages, disabling fragmentation and setting the size limit for ICMPv6 messages.
- ICMPv6 extension header protection. This includes checking the sequence of extension

headers, the number of extension headers, the count of extension headers, and prohibiting certain types of extension headers (Hop-by-Hop Options Header, Destination Options Header, Routing Header, Fragment Header, ESP Option Header, AH Option Header, and None Option Header).
- IPv4 SYN Cookie and IPv6 SYN Cookie.

As common attack methods are mixed with a large number of combined flood attacks, attackers are actually consuming the performance resources of the attacked party. Therefore, the powerful performance support of the firewall system ensures that it will not become a bottleneck in the user's network when a large number of attacks consume the firewall's performance, providing a solid performance foundation for the firewall's attack protection module and other modules.

3.11.3 Advanced multi-dimensional dynamic feature anomaly detection engine

The firewall adopts a brand-new and advanced multi-dimensional dynamic feature anomaly detection engine, discarding the previous static expression method of abnormal behavior feature codes. It refines the feature codes of abnormal and malicious behaviors through multiple dimensions and expresses them dynamically, making the feature expression more comprehensive, precise and effective. This greatly improves the hit quality of the firewall's intrusion prevention system and solves the problem that traditional devices have a high detection hit rate but also a high false alarm rate.

3.11.4 Flexible custom vulnerability/spyware signature feature function

The firewall supports custom definitions for vulnerabilities and spyware based on TCP, UDP and HTTP protocols based on the message structure of each protocol, specify the characteristic values of one or more fields. These characteristic values can be matched in the form of text or regular expressions, and it also supports whether to match and detect these characteristic values in sequence. It supports customizing the source port range and destination port range of vulnerabilities and spyware.

3.11.5 Multi-dimensional DLP Data Leakage Prevention

Firewalls offer content filtering, file filtering, URL filtering, and network behavior management functions. The user's network behavior is being managed and controlled. The behavior control strategy not only supports precise control down to the IP address but also to the user level. Additionally, in content filtering, protection against the leakage of sensitive information has been implemented.

Content filtering supports content filtering based on common protocols and applications.

- Support keyword-based content filtering. Keywords support text matching or regular expression matching

- The protocols include: FTP, HTTP, SMTP, POP3, IMAP, and SMB.

- File types include: html, txt, doc, docx, xls, xlsx, ppt, pptx, pdf.
- RTF, XML, TEX, CHM, SXC and PS.
- File filtering supports file filtering based on common protocols and applications.
- The protocols include: FTP, HTTP, SMTP, POP3, IMAP, and SMB.
- Supports over 30 file types, including: html, doc, docx, xls, xlsx, ppt, pptx, pdf, troff, rtf, xml, tex, mime, pst, hlp, chm, h1s, umd, wdl, cebx, sxc, fdf, tnef, mbx, zip, gz, rar, 7z, bz2, cab, ps, tar, cpio, deb.
- Support scanning and filtering of compressed files, with a maximum of 6 decompression layers.
- Behavior control supports the management of key commands and keyword contents for HTTP, SMTP, POP3, IMAP, FTP, and TELNET protocols, and allows for the setting of sender and recipient address blacklists and whitelists for SMTP, POP3, and IMAP email

protocols.

3.11.6 WAF Function for Web Attacks

The firewall supports professional WAF functions. It has a built-in Web application protection feature library, including various common Web protection application rules. It can provide Web attack protection against "other attacks", "cross-site scripting", "SQL injection", "file inclusion", "directory traversal attacks", "sensitive information leakage", "code execution vulnerabilities", "command line execution vulnerabilities", "upload vulnerability exploitation" and "Web scanning" types of attacks.

Web attack protection of the firewall can support:

- Hide the Server field and X-powered-By field in the HTTP response header, and also support the checking and replacement of 5XX and 4XX error codes.
- URL access control.
- CSRF protection / URL anti-hotlinking.
- Webshell rule checking, Webshell file detection and file type control.
- HTTP anomaly protection, including duplicate detection of Accept-Charset, duplicate detection of Content-Type, value detection of Content-Length field, abnormal detection of URL length, and abnormal detection of field length in HTTP headers.
- Blacklist filter the IP addresses in the X-Forwarded-For field of the HTTP extended header
- HTTP protocol password protection against brute force cracking.
- Anti-scanning, including 302 page anti-scanning, 404 page anti-scanning and directory access frequency detection.

3.11.7 Vulnerability scanning for reinforcing the defense line

The firewall supports vulnerability scanning services for the device operating systems, web applications and Internet of Things in the user's network. It detects vulnerabilities in the user's devices through vulnerability scanning and provides suggestions for vulnerability repair. By strengthening the system, the protection capability is enhanced, thereby preventing attacks targeting the same vulnerabilities.

3.11.8 Powerful threat intelligence penetration

The firewall supports a powerful local threat intelligence detection function, facilitating the detection and identification of unknown threats in the user's network.

Threat intelligence can only be produced based on massive amounts of data relying on QAX automated data processing technology that is based on artificial intelligence self-learning, and multiple domestic high-level security research laboratories with top-notch research resources, provides professional and high-level technical support for the final confirmation of unknown threats.

- All unknown threats identified through big data analysis will be subject to manual intervention by professional personnel for detailed analysis to confirm the attack methods, targets and purposes.
- By integrating artificial intelligence with big data knowledge and multi-dimensional features of attackers, a comprehensive profile of the attackers is reconstructed, including the form of the program, homologous Trojan programs with different coding styles and attack principles, malicious servers (C&C), etc. Through the comprehensive feature 'tracking' of attackers, unknown threats are continuously discovered. Ultimately, the accuracy of the discovered unknown threats is ensured, and threat intelligence available for terminal platforms is generated.

3.12 Multi-system coordinated protection, establishing a three-dimensional protection system

The firewall supports interworking with systems such as the terminal management system, SkyEye, NGSOC, ITS, honeypot, and security cloud, to achieve three-dimensional and full-network behavior detection and security protection based on "cloud-border-end", and to locate and block both known and unknown threats.

3.12.1 Firewall and terminal system interaction

The firewall supports integration with the terminal management system, terminal identification center, and terminal NAC to achieve terminal control, private cloud virus scanning and killing, and terminal access control functions.

- Terminal control: The firewall integrates with the terminal management system to implement terminal control based on the security scan results of user PC terminals provided by the terminal management system. This control is executed according to the risk levels of user terminals, categorized as high, medium, and low. Furthermore, it supports the management of terminals that do not have the Qianxin Security Assistant installed, thereby ensuring a high coverage rate for antivirus software installation.
- Private cloud virus detection and elimination: The firewall, in conjunction with the terminal identification center, transmits the MD5 hash of unknown files to the terminal identification center for analysis, utilizing the cloud-based virus database to improve the virus detection rate.

- Terminal access control: The firewall and terminal NAC can be integrated to leverage the firewall's precise control capabilities to finely manage users' network access behaviors, thereby achieving functions such as access control for core business, compliance with network security requirements, real-name authentication management for network access, and security protection for network boundary access.

3.12.2 Firewall and SkyEye System Integration

The firewall supports integration with the SkyEye analysis platform and SkyEye sandbox, combining the in-depth detection capabilities of SkyEye with the real-time blocking capabilities of the firewall to achieve functions such as threat detection, one-click handling, and sandbox linkage.

- Deep detection:The firewall, in collaboration with the SkyEye analysis platform, uploads the traffic passing through the firewall in the form of logs to the SkyEye analysis platform for in-depth detection and analysis, fully leveraging the deep detection capabilities of SkyEye.
- One-click response: After receiving the firewall logs, SkyEye conducts in-depth analysis. Once a threat is detected, it automatically or manually issues a response strategy. The firewall supports the response strategies issued by the SkyEye analysis platform to handle and block the detected threats, thereby providing security guarantees for users' outbound traffic.
- Sandbox integration: The firewall supports integration with the Skyeye sandbox, sending unknown threat files to the sandbox for detection and responding to the sandbox's detection results to handle and block unknown viruses discovered by the sandbox. As a supplement to the local and cloud virus databases, the sandbox can significantly enhance the firewall's virus protection capabilities, especially for unknown viruses.

3.12.3 Firewall and NGSOC System Integration

The firewall supports integration with the NGSOC system, leveraging the NGSOC system's data deep mining and situation awareness capabilities to achieve visualization of the user network status and threats. At the same time, it supports responding to the disposal strategies issued by the NGSOC platform to complete one-click threat handling.

- Situation awareness. The firewall supports uploading the collected network traffic in the form of logs to the NGSOC platform for in-depth analysis. Combined with the deep data mining of NGSOC, it realizes visualized situation awareness.

- The firewall supports the response to the disposal strategies of the NGSOC platform, completing the handling and interception of discovered threats, thereby providing security guarantees for the network traffic of user access.

3.12.4 Firewall and Security Cloud System Integration

As a cloud-based large database, the capacity and real-time status of the Security Cloud are beyond the reach of a single firewall.

The firewall supports integration with the security cloud, using the cloud-based URL library, virus library, application identification library and other resources as supplements and expansions to the local libraries of the firewall, thereby enhancing the depth and breadth of identification for applications and threats.

Meanwhile, for unknown viruses, it also supports uploading to the cloud sandbox for identification.

3.12.5 Firewall and honeypot integration

The firewall supports network deception technology, which can detect scanning activities in the network and lure suspicious traffic to honeypots for in-depth interaction detection and analysis. Based on the analysis results, it can block the discovered attack traffic, thereby protecting the existing business network.

The honeypot linkage function supports multiple trapping methods including static trapping based on five-tuple, dynamic trapping based on non-existent IP addresses, dynamic trapping based on non-existent ports, and malicious domain name trapping based on IOC. Depending on the deployment location of the firewall, it is possible to trap public network traffic or internal network traffic.

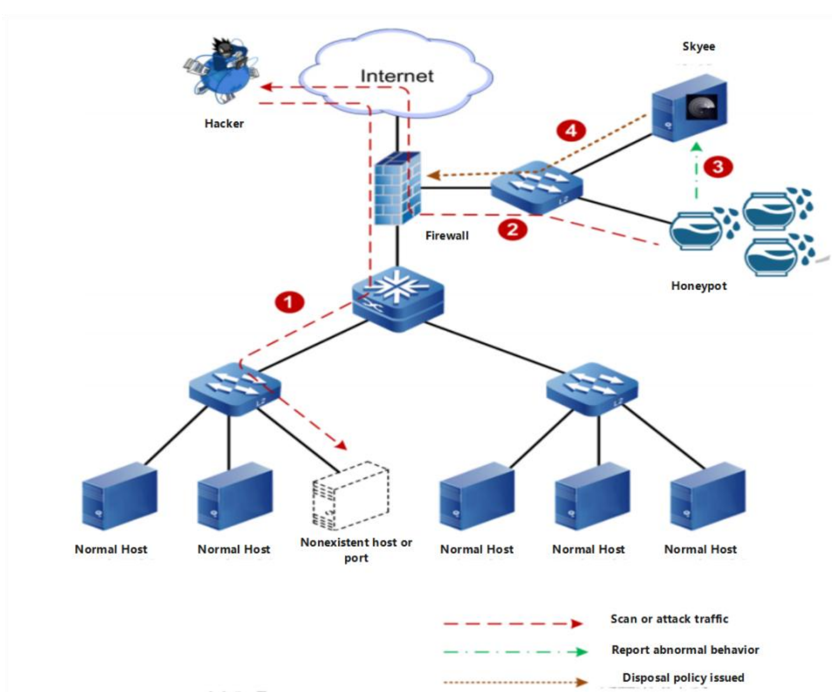


Figure 3-27 Trapping Implementation Process - Public Network

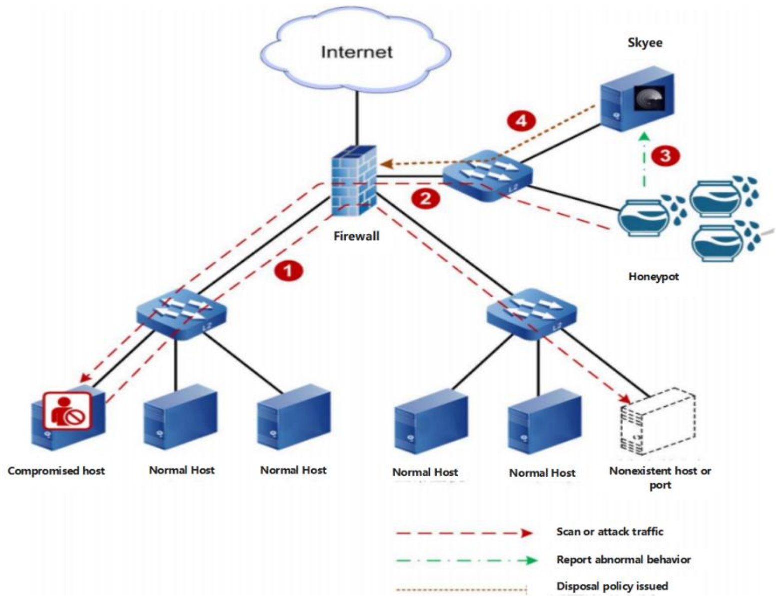


Figure 3-28 Intranet Trap Implementation Process

- Hackers conduct IP address scans or TCP port scans on users' networks.
- When the firewall detects scanning behavior, it lures the suspicious traffic to the honeypot for attack detection. The honeypot simulates multiple services such as HTTP/SSH/SMB/RDP, responds to the hacker's scanning behavior, and interacts deeply with them. It analyzes the hacker's behavior, identifies the attack tools, and records various application layer attack methods and abnormal behaviors of the hackers.

- The honeypot reports the logs of abnormal behaviors to the SkyEye analysis platform.
- Users can analyze abnormal behaviors on the SkyEye Analysis Platform. After the administrator confirms the abnormal behavior, they can issue disposal strategies to the firewall on the SkyEye Analysis Platform.
- The firewall receives the coordinated response strategy, disconnects the attack source, and protects the business network.

3.13 Application and traffic visualization, network behavior nowhere to hide

3.13.1 Overview

The firewall can identify over 7,000 application protocols and supports manual addition of specific applications. It also supports deep content inspection technology and can recognize applications without professional configuration.

Users who need to know the detailed bandwidth usage can do so by accessing the data center of the firewall.

Classification	Content Supported for Audit
Internet Traffic Audit	Includes the destination IP address, destination port, application, and traffic volume of the user's access.
DNS Resolution Audit	Mainly audits the DNS resolutions carried out by users, including domain names and the addresses after domain name resolution.
Instant Messaging Audit	Includes the audit of IM login and logout behaviors, including login/logout status and IM numbers.
Illegal Content Audit	Supports content audit based on keywords, including the audit of illegal content in users' web browsing, file upload/download, and email sending/receiving.

Illegal File Audit	Supports the filtering and audit of files, including the audit of users' uploading and downloading of files in illegal formats.
Malicious Behavior Audit	Supports the audit of malicious behaviors, including attacks, virus protection, and Trojan protection.

3.13.2 High-capacity and multi-dimensional diary

The firewall's log module records multi-dimensional details of user Internet behavior and content, including time, content, application, location, threat, and security domain, in addition to the traditional five-tuple. With over 45 dimensions, it ensures robust log analysis and statistical capabilities.

3.13.3 Diverse log retrieval methods

The firewall log module supports precise and fuzzy filtering based on keywords, and offers a variety of filtering conditions such as AND, OR, NOT, greater than, equal to, not equal to, and negation. It enables quick search by single-click selection on the log interface. It also supports custom configuration of search conditions and collection of these conditions for convenient and rapid use

3.13.4 Comprehensive risk information display and analysis

The firewall provides users with comprehensive and real-time risk information display, highlighting compromised hosts, threat events, and key objects of concern, and offers one-click access to the abnormal behavior tracking interface.

The firewall configuration threat analysis module can precisely locate the traces of abnormal behavior through fuzzy search with custom keywords. Coupled with all-round monitoring and analysis of vulnerabilities, applications, sessions, and networks, it can confirm whether the abnormal behavior poses a risk.

3.13.5 A powerful content auditing function

The firewall supports powerful and flexible content auditing, file auditing and malicious behavior auditing policies.

- **Content auditing**

The system supports predefined keyword groups, including email addresses, MD5, mobile phone numbers, ID card numbers and bank card numbers. At the same time, it supports administrators to define their own keyword groups. Administrators can define the keywords that need to be filtered or audited through regular expression matching or text matching.

Administrators can also configure flexible keyword hit counts. In a more lenient setting, a keyword can be hit multiple times before being recorded; in a stricter setting, it will be recorded after just one hit.

- **File Audit**

The system supports the control and auditing of specified types of files, including HTML, DOC, XLS, PDF, RAR and many other file types. The system does not manage and control network based on file extensions, so changing the file extension cannot evade the auditing and control of the firewall.

The system supports control and auditing of compressed files, and can manage compressed files that have been compressed up to six times.

- **Malicious behavior audit**

The system supports the configuration of fine-grained behavior auditing policies, including various common attacks, viruses, Trojans, etc.

3.14 Automated emergency response function

The response time window during an emergency cybersecurity incident directly determines the extent of threat spread and the magnitude of asset loss. Therefore, emergency response is the most crucial aspect of cybersecurity.

The firewall supports an automated emergency response function. This function, in response to hot intrusion prevention events and threat intelligence events, issues notifications from the cloud and the firewall automatically implements defense measures. This reduces the time delay caused by manual response and operation, thereby preventing network compromise.

During emergency response, the security cloud issues emergency response notifications uniformly. Upon receiving the notification, the firewall automatically

Check whether the local license, IPS library version and intrusion prevention policy are normal. And automatically or manually execute the protection policy to complete the protection against critical threat vulnerabilities

4 Technical advantages

4.1 Adopting the fourth-generation SecOS system

The fourth-generation SecOS operating system of Topsec, which enjoys full independent intellectual property rights, builds on the high security, high openness, high scalability and high portability brought by the third-generation SecOS. It focuses on enhancing the firewall's collaborative defense capabilities, data generation capabilities, data analysis capabilities and data handling capabilities, enabling the firewall to achieve multi-terminal linkage, all-round display of risk information, interception of known threats, location of unknown threats and one-click operation.

The ability to handle threatening behaviors makes up for the shortcoming of traditional firewalls that focus more on reconfiguration than management, and can provide multi-dimensional effective information to help users complete daily maintenance work.

4.2 The overall framework adopts an AMP+ parallel processing architecture.

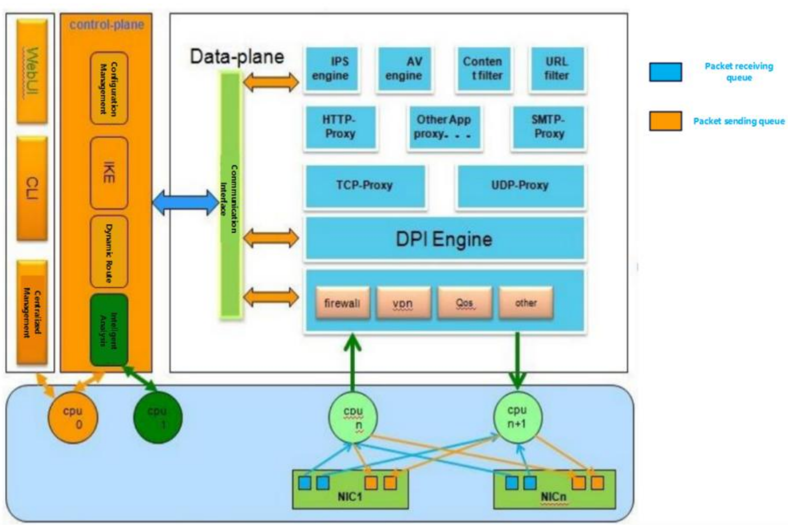


Figure 4-1 Overall Framework of the Firewall System

The overall framework of the firewall system adopts the AMP+ architecture, which is a more optimized multi-core asynchronous parallel processing architecture. The overall architecture is divided into three major parts:

- Configuration management plane: handled by CPU0.
- The control plane is handled by CPU0, while the intelligent analysis function is processed by CPU1.
- The data plane is processed by the remaining CPUs on an average basis.

Under the AMP+ architecture, multiple planes are responsible for different tasks, achieving a layered, independent, and asynchronous concurrent working system. This has brought a revolutionary improvement to the performance of the firewall system. The three-layer separation of the configuration management plane, control plane, and data plane ensures the overall stability and reliability of the firewall.

4.3 The optimized AMP+ architecture breaks through the bottlenecks of the traditional SMP architecture.

The traditional SMP architecture enables concurrent processing under multi-core conditions. The same task, "Task One", is assigned to different CPUs, as shown in the following figure.

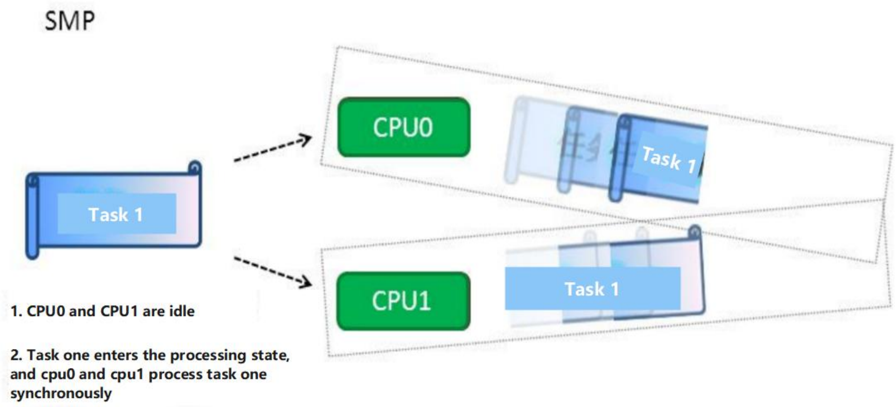


Figure 4-2 Task Processing Diagram of Traditional SMP Architecture 1

When one of the CPUs is occupied by another task, "Task Two", the remaining CPUs that are processing "Task One" will be in a waiting state due to the lock on "Task One", which reduces CPU efficiency and prolongs the task processing time, as shown in the following figure.

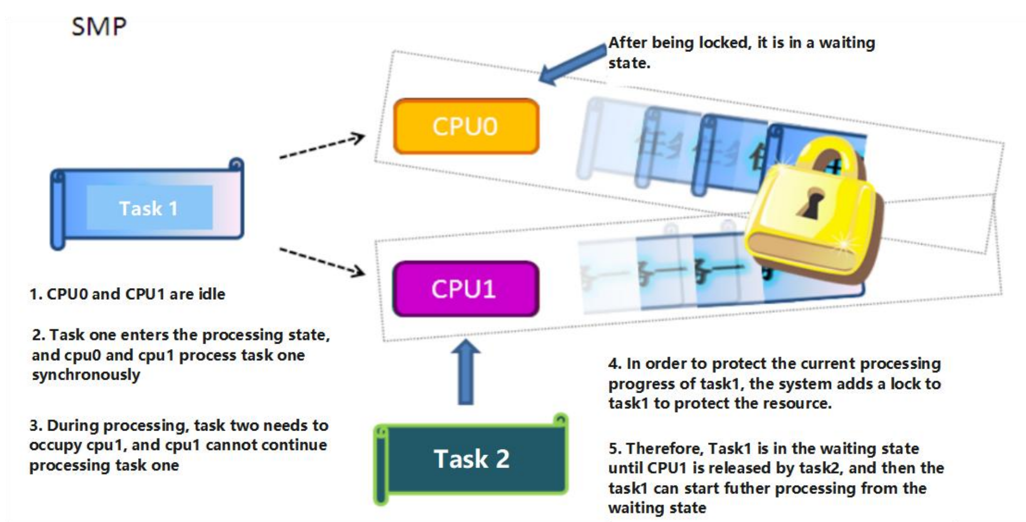


Figure 4-3 Task Processing Diagram of Traditional SMP Architecture 2

The firewall system adopts the AMP+ architecture, which is an asynchronous parallel processing architecture. Different CPUs can handle different tasks, which greatly reduces the situation where tasks are locked, breaks through the bottleneck under the SMP architecture, improves the efficiency of the CPU, and significantly shortens the task processing time. Thus, the overall processing speed of the firewall is accelerated. As shown in the following figure.

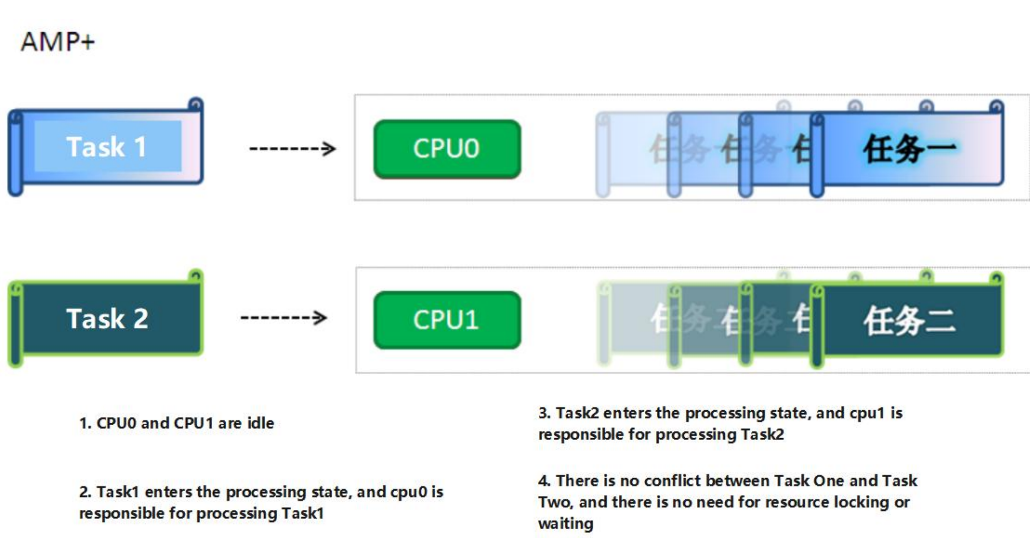


Figure 4-4 Task Processing Diagram of AMP + Architecture for Firewall System

4.4 Optimized processing of data transmission and reception through network ports

Take the processing of network port data reception as an example. In the traditional multi-core architecture, in order to achieve multi-core parallel processing, the CPU is bound to the network port.

As can be seen from the above figure, in the traditional multi-core architecture, when the network interface does not receive any data, the CPU bound to it will be in an idle state, and the CPU utilization rate has not been maximized.

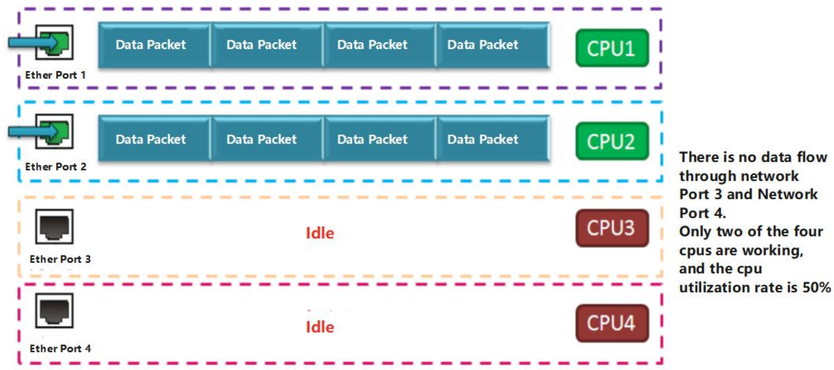


Figure 4-5 Data Processing Diagram of Network Ports in Traditional SMP Architecture

The AMP+ architecture adopted by the firewall system has optimized processing. The CPU is no longer bound to the network interface. Instead, the receive and transmit packet queues of the network card are evenly distributed to each CPU based on the number of CPUs in the data plane. This ensures the parallelism of the data plane CPUs and maximizes CPU utilization.

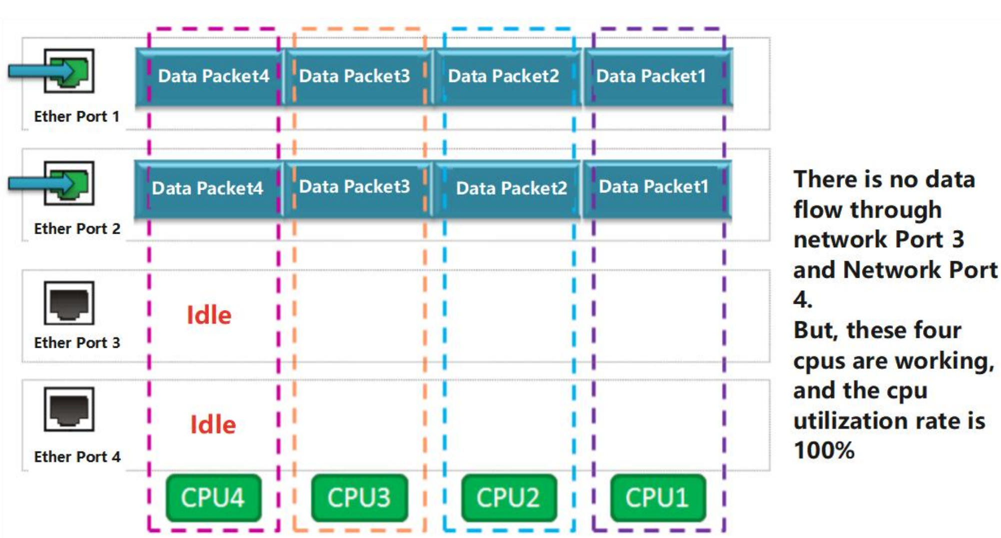


Figure 4-6 Data Processing Diagram of Network Ports in Firewall System

From the above structure picture, As long as any one of the network ports receives data, all the CPUs will be in operation, and the CPU utilization rate reaches its maximum.

4.5 Single-engine one-time data processing technology

Most traditional firewalls or UTM technologies are based on the Linux system. The basic data forwarding function is implemented in the Linux kernel, while advanced security functions (such as IPS, anti-virus, content filtering, etc.) are carried out in the user space. This results in the data needing to be transferred from the kernel to the user space when advanced protection is in operation, processed there, and then sent back to the kernel before being sent out.

This approach has three major drawbacks overall:

- Frequent up and down transmission of data packets.
- Frequent switching between processes
- The conversation cannot be reused.

After the firewall system adopts the integrated engine technology, the data processing flow is as shown in the following figure.

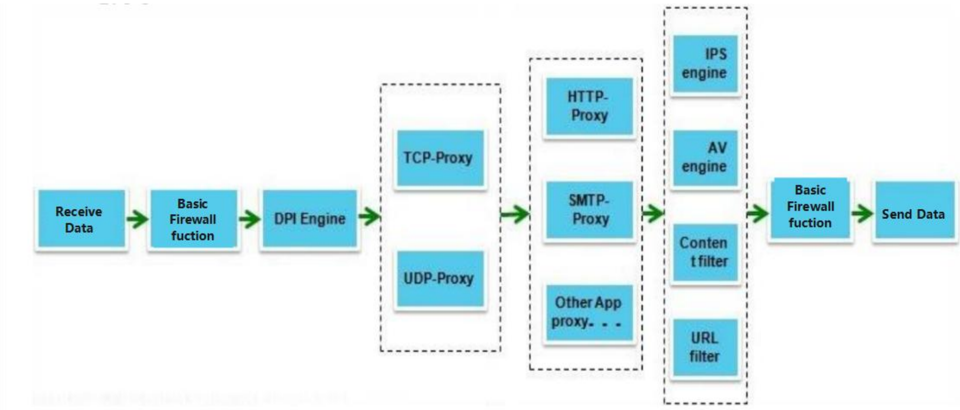


Figure 4-7 One-time Data Processing Diagram of Firewall System with a Single Engine

From the figure, The entire process of data reception, data processing (including application layer data processing, IPS, anti-virus and other advanced functions), and data transmission are all completed in the data plane, without involving issues such as data packet copying and process switching. Meanwhile, the same session is used throughout the entire forwarding stage for data processing. This significantly enhances the processing speed at the application layer and reduces the overall latency of data forwarding.

4.6 Multi-level redundant architecture enhances the reliability of firewalls

The firewall supports multiple multi-level redundancy architectures, enhancing the reliability of the firewall, including:

1) Redundant architecture of the firewall data plane. As the tasks of receiving and sending network port data are evenly distributed to each CPU for processing, when one or more CPUs fail to work, the remaining CPUs can still operate normally. Since the tasks of receiving and sending data are still evenly distributed to each currently operational CPU, this enhances the reliability of the firewall on the data plane.
2) Redundant architecture of the firewall system. The firewall supports the import of two systems, and these two systems are independent of each other. When the system currently in use by the user encounters a problem, the user can switch to the other system. This enhances the reliability of the firewall at the system level.
3) Redundant architecture of firewall network links. On the firewall system, the enhanced SGRP (Single Gateway Redundancy Protocol) is adopted to achieve dual-master routing load balancing and master-standby routing redundancy backup modes. It also supports HA (High Availability) redundancy backup and rapid switching in transparent environments. This enhances the reliability of the firewall on the network links.

4.7 User-space Protocol Stack based on multi-core parallel architecture

Design a high-performance forwarding platform through an architecture that separates the data plane from the control plane. The configuration and negotiation of network protocols are completed in the control plane, while the network data interaction part, ESP, SSL and other application layer data, as well as security detection (IPS/AV/URL) functions are accomplished in the data plane

The user-space protocol stack directly maps the network card queues to memory through technologies such as UIO and DMA, allowing the application forwarding protocol stack program to directly read from memory to reduce the number of message copies; it enhances the efficiency of CPU reading data from the cache through techniques like large pages and cache lines; and it improves the efficient operation of user-space programs by means of pre-allocated memory pools, reducing system calls, disabling interrupts, CPU affinity, and lock-free queues. In summary, these methods are employed to enhance the system's forwarding processing performance, including SSL session counts.

4.8 Cloud-based collaborative expansion for precise threat location

In addition to the built-in intrusion prevention, virus, URL and application recognition feature libraries, the firewall can also be linked with the security cloud, which provides functions such as cloud-based virus scanning and killing, URL cloud recognition, application cloud recognition and cloud sandbox.

This expands the firewall's signature library, accurately locates threats in the network, and works in conjunction with the disposal center to handle confirmed threat behaviors.

4.9 Closed-loop Defense against Unknown Threats Based on NDR Security System

For traditional security, the focus has been on addressing known threats. While Qianxin Group supplements the deficiencies of traditional security and enhances the efficiency of identifying known threats, it also contemplates new branches of future cybersecurity development.

In recent years, the continuous increase in the value of information has exposed enterprises' data security to more threats and deeper impacts. Traditional security measures, which address known threats, cannot truly protect users' data security. Advanced threats can often bypass various traditional security defenses through compliant data and successfully achieve the goal of data theft. Therefore, we urgently need a new security system to prevent unknown threats.

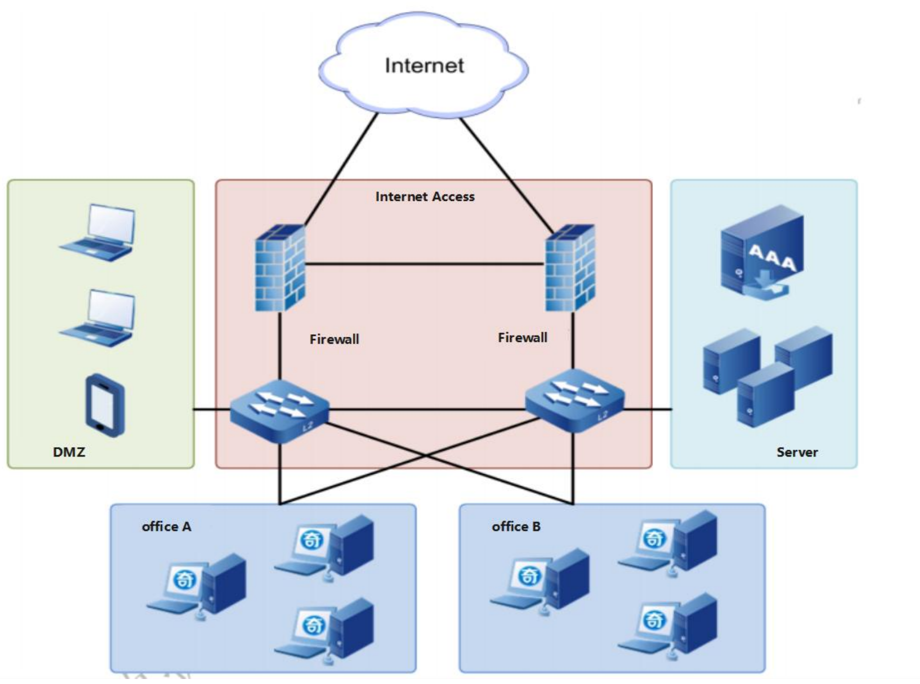
Combining the accumulation of big data mining technology and data security analysis, Qianxin Group has established a network-based detection and response system (NDR for short) driven by big data. It has formed a defense loop based on the Internet and the user's own network, which includes dynamic data detection, dynamic behavior detection, and dynamic response and handling for unknown threats.

As an essential component of the NDR security system, the firewall system utilizes the identification of data and behavior within the user's own network, combined with cloud-based detection of known threats based on features, unknown threats based on sandboxes, discovery of compromised hosts based on threat intelligence, and detection of unknown threats based on security models. It also integrates multi-dimensional correlation analysis and progressive data drilling of firewalls/SMACs to visually track, locate, and handle unknown threat behaviors, completing one-click handling and policy optimization of unknown threats, as well as the traceability of security incidents.

5 Typical application scenarios and value

5.1 Enterprise Internet Boundary Security Application Scenarios

5.1.1 Typical scenarios

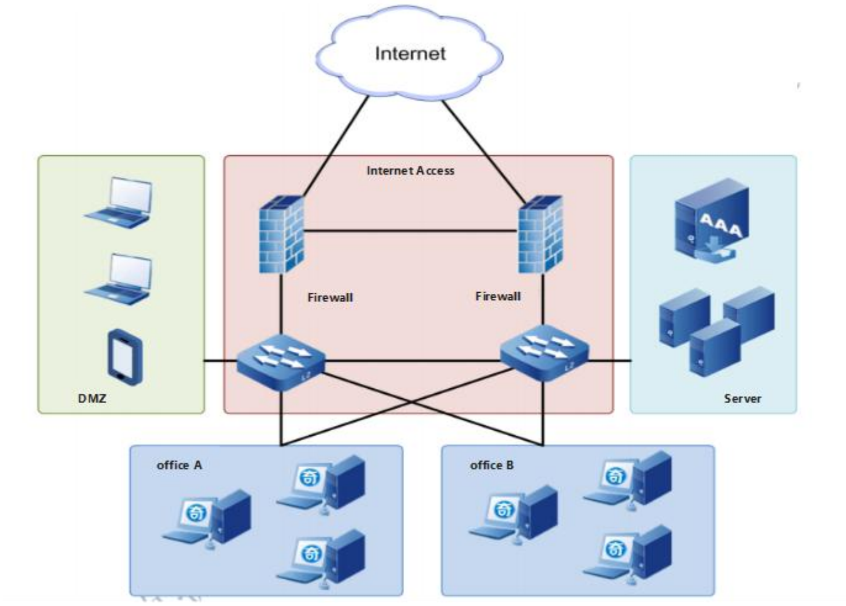


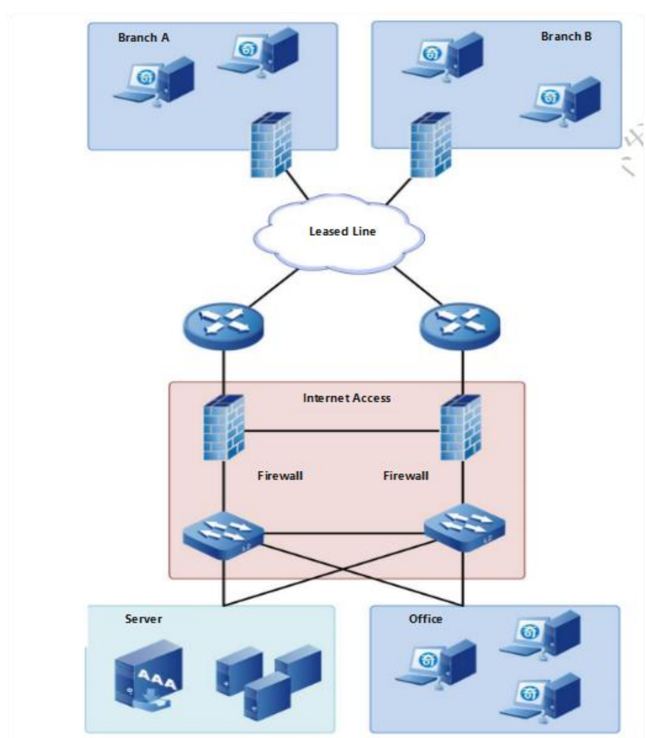
5.1.2 Requirement and advantages

Requirement	Advantages
There are many external threats, and the cybersecurity awareness of Internet users should be taken into consideration	It is linked with the terminal relationship system to achieve unified management of user terminals in accordance with security
The composition of internal network traffic is complex	Comprehensive and robust application-level integrated security protection
Key business guarantee requires attention to the bandwidth and behavior of Internet access	Adjust the bandwidth dynamically as needed

5.2 Cybersecurity application scenarios for industry-specific private networks

5.2.1 Typical scenarios



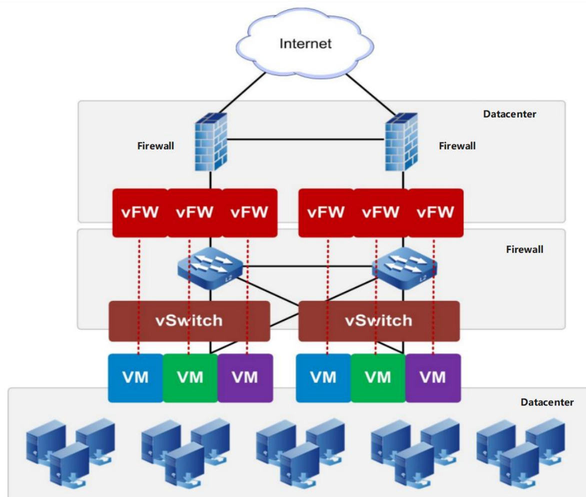


5.2.2 Requirement and advantages

Requirement	Advantages
Multi-link backup to improve network availability and efficient dual hot standby	Efficient dual hot standby
Multi-branch interconnection to ensure business security transmission	Standard IPSecVPN, SSL VPN function
To ensure the normal operation of key businesses, it is necessary to impose constraints on network bandwidth and behavior.	Adjust the bandwidth dynamically as needed
Internal network traffic components are complex,	Provide comprehensive and robust application level integrated security protection
There are many external threats, and the network security awareness of Internet users is different	It works with terminals to enhance the accurate identification of Trojans and applications, fine-grained control of user terminals according to security risks, and realizes network access and access control with NAC

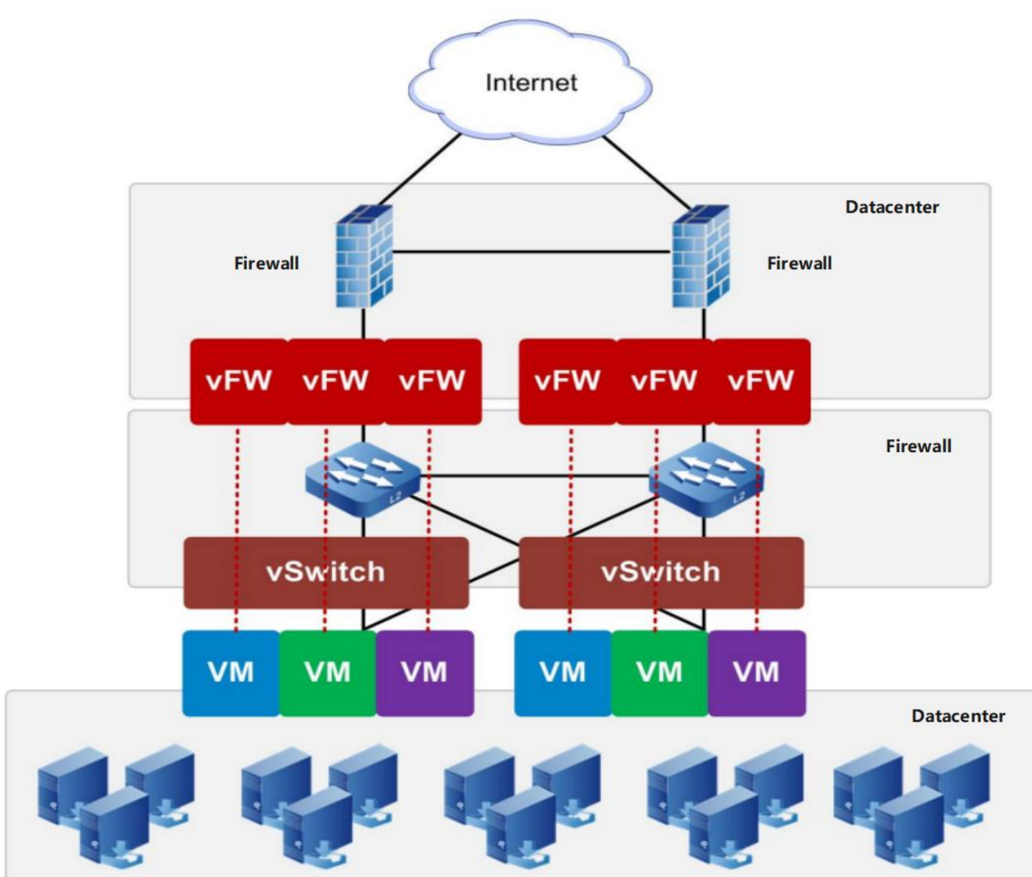
5.3 Data Center Exit Security Application Scenarios

5.3.1 Typical scenarios



5.4 Multi-branch enterprise networking security application scenarios

5.4.1 Typical scenarios



5.4.2 Pain points and advantages

Requirement	Advantages
Multi-branch interconnection ensures the secure transmission of each branch	Intelligent firewalls are deployed at the exit, and VPN is established between branches and headquarters to realize backup and load of links, and secure border

	isolation and Internet threat attack defense
Headquarters/branch integrated defense strategy, security control of external access	Deep threat detection is carried out on the whole network traffic, and the local threat intelligence is used to analyze the suspicious behavior in depth to block the spread of viruses, vulnerability intrusion, and real-time early warning to block high concealment threats
Terminal security is guaranteed to prevent the whole network risk caused by a single terminal being breached	Cooperate with Tianqing to achieve gateway and local virus killing, as well as access control based on terminal risk
Unified management, status monitoring and data analysis of multiple firewalls	SMAC system was deployed to build a centralized management and analysis platform that integrated configuration batch distribution, state unified monitoring, and failure host early warning

6 Prospects for technological development trends

The future firewall is evolving in three major directions: visualization, intelligence, and software.

- Visualization

Firewalls themselves generate a large amount of logs every day. These log data cannot directly display the anomalies and correlations within them, making it difficult for users to quickly identify abnormal and attack behaviors. Currently, all firewalls are beginning to have visualized data charts, which display the key information and associated data in the logs that are useful to users through a visual approach.

- Intelligent

The intelligence of firewalls includes new technologies such as software-defined firewalls, enabling users to issue instructions through humanized language, thus making the use of firewalls more user-friendly and humanized.

- Software-based

With the development of big data and cloud computing, firewalls have gradually evolved from specific hardware products to support virtualized deployment on cloud platforms, thus meeting the security needs of cloud data. In the future, they can support on-demand purchase and allocation, eliminating the need for users to deploy them separately and saving a significant amount of funds.