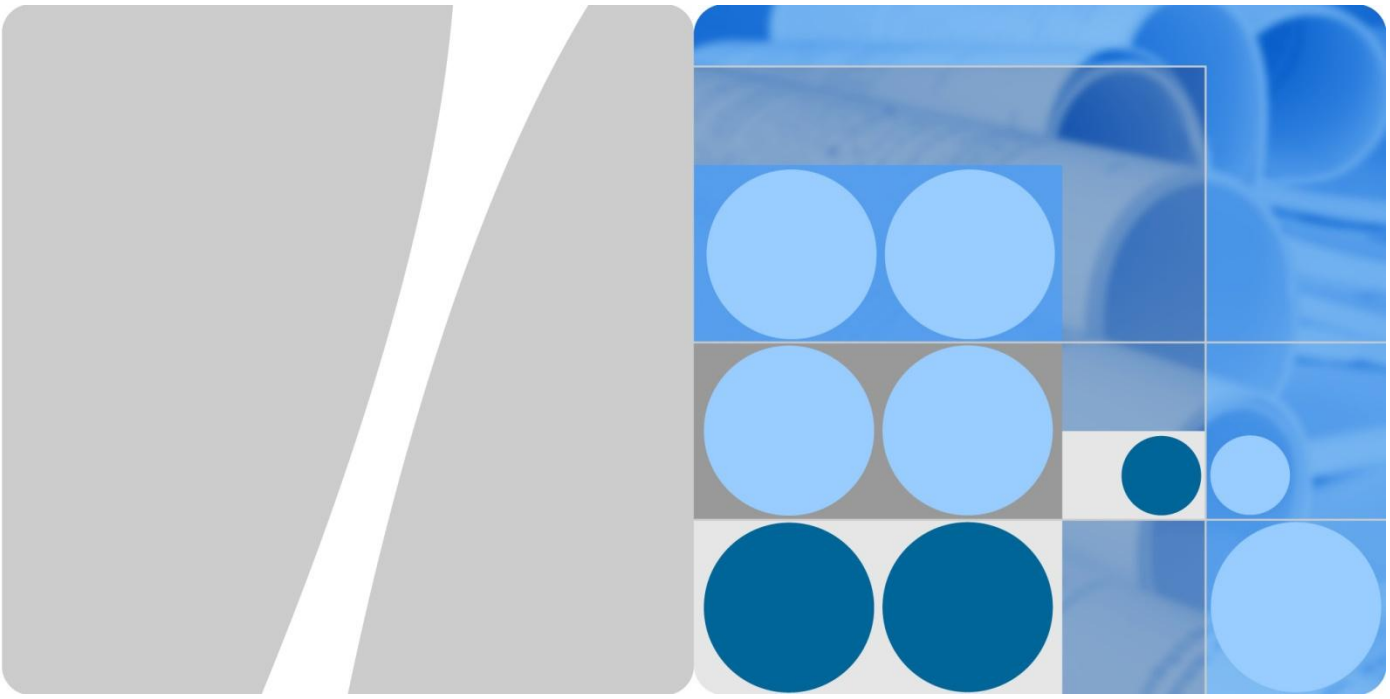


HUAWEI USG6000 Series Next-Generation Firewall Technical White Paper — VPN

Issue 1.1

Date 2014-03-14

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

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

Website: http://enterprise.huawei.com

Email: ask_FW_MKT@huawei.com

Key Words

NGFW, VPN, IPSec, IKE

Abstract

This document describes the characteristics and principles of NGFW IPSec VPN and SSL VPN technologies.

Acronyms and Abbreviations

Abbreviation	Full Spelling
NGFW	Next Generation Firewall
VPN	Virtual Private Network
IPSEC	IP Security
IKE	Internet Key Exchange

Contents

1 Technical Background

As network economy develops and enterprises expand, enterprises have more customers and partners. This situation prompts profit growth but highlights the functional defects of the traditional enterprise networks. Leased-line connections based on fixed physical locations can hardly meet the communication needs of modern enterprises. For their own network construction, enterprises have higher demands in terms of network flexibility, security, cost-effectiveness, and scalability. The virtual private network (VPN) can meet the demands as it requires less network operation and maintenance and helps enterprises achieve commercial goals.

VPN is a recently popularized technology dramatically developed with wide Internet application. It helps construct virtual private networks on a public network. "Virtual" indicates logical networks. VPNs are deployed between enterprises or between enterprise branches for secure and cost-effective connections.

The basic VPN principle is to use tunneling technologies to encapsulate packets into tunnels and construct private data transmission tunnels over backbone networks to transparently transmit data packets. A tunneling technology uses one protocol to encapsulate the packets of another protocol. The encapsulation protocol can be encapsulated or carried by other protocols.

VPNs have the following characteristics:

Private: VPN users have the same experience as traditional network users. VPN resources are independent of those for bearer networks. That is, only the users of a VPN can use its resources. In addition, each VPN protects internal information and prevents others from accessing the information.

Virtual: VPN users communicate over a public network (VPN backbone network) that non-VPN users may use. To be specific, the private network for VPN users is a logical network.

Huawei NGFW series supports the following types of VPNs:

- IPSec VPN

  As defined by the IETF, IPSec provides a method for establishing and managing secure tunnels. By authenticating and encrypting data packets, IPSec prevents packet interception or tampering during packet transmission on private and public networks. In a word, IPSec creates a secure communication tunnel for users in different areas.
- L2TP VPN

PPP allows the packets of various protocols to be transmitted on Layer-2 P2P links. In this case, PPP is running between a user and the NAS, with both one end of the Layer-2 link and PPP session endpoint on the same device.

The Layer 2 Tunneling Protocol (L2TP) supports PPP frame transmission over tunnels, allows Layer-2 links and PPP sessions to originate from different devices, and uses the packet exchange technology for information interaction. L2TP extends the PPP pattern.

- GRE VPN

  The Generic Routing Encapsulation (GRE) technology encapsulates the packets of one network-layer protocol, such as Internet Packet Exchange (IPX), so that the packets can be transmitted over other another network-layer protocol, such as IP. GRE can serve as the Layer-3 tunneling protocol for a VPN to provide transparent transmission channels for VPN data.

  IPSec can be used to encrypt GRE packets for security.

- SSL VPN

  A Secure Sockets Layer (SSL) VPN does not require client installation. Users can use HTTPS-enabled Web browsers to establish standard secure channels to access remote applications. This mechanism significantly decreases the VPN system management workload. SSL VPNs apply to the following situations:

  - Enterprises need to access the Internet.
  - Firewalls are deployed between servers and clients to allow HTTPS not IKE or IPSec packets to pass.
  - Fine-grained access control is needed.

Huawei NGFW series uses the IPSec mechanism to provide services, such as access control, connectionless integrity, data source authentication, anti-replay, and flow-classification-based encryption. The NGFW series uses Authentication Header (AH) and Encapsulating Security Payload (ESP) security protocols to protect IP or upper-layer data. IPSec provides the following types of network security services:

Privacy: IPSec encrypts packets before transmitting them for data confidentiality.

Integrity: IPSec verifies packets at the destination against data tampering during transmission.

Authenticity: IPSec authenticates all protected packets.

Anti-replay: IPSec prevents packets from being captured or retransmitted on the network. That is, the destination denies duplicate packets. Sequence numbers help implement anti-replay.

Huawei NGFW series uses IPSec VPNs to establish VPN tunnels between the headquarters VPN gateway and branch VPN gateways and obtain private addresses for secure transmission. IPSec provides protection for data transmission between hosts, between security gateways, or between hosts and security gateways. Multiple SAs can be established between two ends. IPSec uses access control lists (ACLs) and SAs to apply protection policies to data flows for particular protection effects. IPSec SAs can be manually configured, but manual configuration becomes difficult when network nodes increase. In this case, IKE can be used to automatically establish SAs and exchange keys. The IPSec VPN function on Huawei NGFW series provides a certificate authentication mechanism based on the Public Key Infrastructure (PKI).

NGFWs support the following new IPSec features:

- IPSec tunneling

Huawei NGFW series supports IPSec tunneling. IPSec tunneling applies IPSec policies to logical tunnel interfaces and uses static routes to guide the packets that IPSec is protecting to the tunnel interfaces for IPSec processing. Packets received by any common interface can be diverted to tunnel interfaces. After IPSec processing, packets are routed to physical outbound interfaces for link backup. To be specific, if the original physical outbound interface of a packet is Down, the packet can be sent to another physical outbound interface through another route, which prevents IPSec service interruption.

- IPSec hot standby

  In practice, IPSec hot standby is deployed to avoid IPSec service interruption in case one firewall goes Down. IPSec hot standby allows the active firewall to back up IPSec and tunnel configurations to the standby firewall. In this manner, IPSec tunnels remain Up even if the active firewall gets disconnected. This mechanism enhances network reliability.

- IPSec load balancing

  Though IPSec hot standby makes IPSec VPN services stable and reliable, only one firewall is working at a time, wasting resources. Therefore, IPSec hot standby is seldom deployed in real-world situations. As a substitute, IPSec load balancing allows two firewalls to process services at the same time. If one becomes faulty, the other immediately takes over all services, ensuring service continuity.

  IPSec load balancing improves the efficiency of firewall use and perfects the IPSec VPN hot standby solution.

- DSVPN

  More and more enterprises adopt the Hub-Spoke (headquarters-branch) networking model. VPN tunnels are established between the enterprise headquarters and branches. The Headquarters serves as the Hub node, while the branches serve as Spoke nodes. In the traditional Hub-Spoke model, data traffic is transmitted between the headquarters and branches. If branches need to communicate, data packets are transmitted as follows:

  The device in branch A encapsulates data packets and sends the packets through the VPN tunnel to the headquarters.

  The device in the headquarters receives, decapsulates, encapsulates, and sends the packets through the VPN tunnel to branch B.

  The device in branch B receives, decapsulates, and forwards the packets.

  In a word, communication between branches is transferred through the headquarters, increasing transmission delays and burdening the transit node. NGFWs allow VPN tunnels to be established between branches.

  As Spoke nodes dynamically obtain IP addresses to access public networks, one Spoke node must obtain the public IP address of its peer before establishing a VPN tunnel to the peer. DSVPNs use the Next Hop Resolution Protocol (NHRP) to maintain and distribute public IP addresses.

- IPSec QOS

  Traditional network services use best-effort policies to equally process all packets and ignore delay, jitter, packet loss issues or reliability requirements.

  As network technologies develop and services become diversified, new services require higher network service performance.

  These services have special bandwidth and transmission performance (delay, jitter, and packet loss ratio) requirements. For example, video conferencing and video-on-demand request high bandwidth, low delay, and low jitter. Key tasks, such as Transaction and Telnet, request low delay and preferential processing especially during congestion but do not require high bandwidth.

Users of these new services are no longer satisfied that packets are sent to the destination. They look forward to better services, such as dedicated bandwidth, low packet loss ratio, traffic management and control, congestion avoidance, and prioritized packet processing, during packet transmission.

IPSec uses QoS to make some services preferentially enter IPSec tunnels. A firewall performs QoS on packets, encapsulates packets based on the QoS result, and sends the packets through IPSec tunnels.

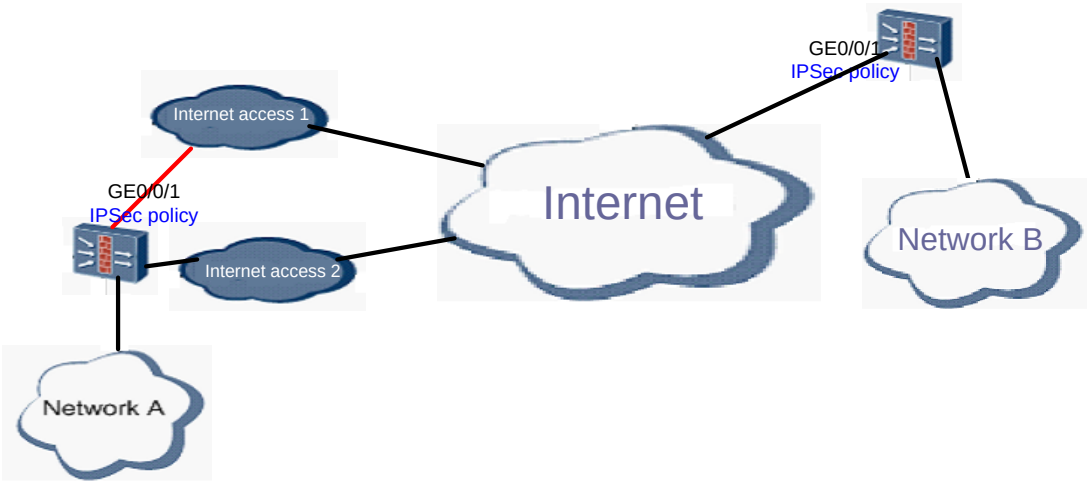
2 Definition and Mechanism

2.1 IPSec Tunneling Concept

IPSec policies are configured on physical interfaces through which packets are sent and received. If a physical link fails, the IPSec tunnel is interrupted.

As shown in Figure 2-1, the firewall connected to network A connects to the Internet through two interfaces and establishes IPSec tunnels to the firewall connected to network B. If one interface fails, the firewall can use the other interface to send traffic.

Figure 2-1 IPSec tunneling application scenario



IPSec tunneling has the following advantages:

- Simplified configuration

  Packets on any physical interface can be routed to tunnel interfaces for IPSec processing, simplifying IPSec policy configuration. Network planning does not affect IPSec configuration, enhancing network planning scalability.
- Flexible service application

  IPSec tunneling is divided into two phases: pre-encryption and post-encryption. You can select a phase to implement other services, such as QoS according to networking requirements.
- Enhanced link reliability

IPSec tunneling implements egress link backup through route configuration, enhancing link reliability.

2.2 IPSec Tunneling Mechanism

Huawei NGFW series supports the application of IPSec policies to both virtual tunnel interfaces (IPSec tunneling) and physical interfaces.

IPSec tunneling provides a simple IPSec tunnel establishment method. IPSec policies are not associated with any physical interfaces. Instead, the policies apply to logical tunnel interfaces, and routes are used to select outbound interfaces and determine the traffic to be encrypted, making IPSec policies flexible and implementing IPSec tunnel backup.

2.3 IPSec Hot Standby Concept

On a live network, an NGFW serves as the network egress and establishes an IPSec tunnel with its peer. If the NGFW fails, the IPSec tunnel is cut off, interrupting services. When IPSec hot standby is deployed, one firewall takes over all traffic if the other fails. Services are uninterrupted, and users are unaware of the firewall failure.

For IPSec hot standby, two independent firewalls of the same model are deployed to provide reliable networking. Of the two firewalls, only one is working at a time. If the active firewall fails, the standby one takes over its services. The active firewall sends its configuration and SA information through the heartbeat interface to the standby one. In this manner, active and standby firewalls maintain the same IPSec information, guaranteeing a smooth service switchover if the active firewall fails.

2.4 IPSec Hot Standby Mechanism

Figure 2-2 IPSec hot standby data flows

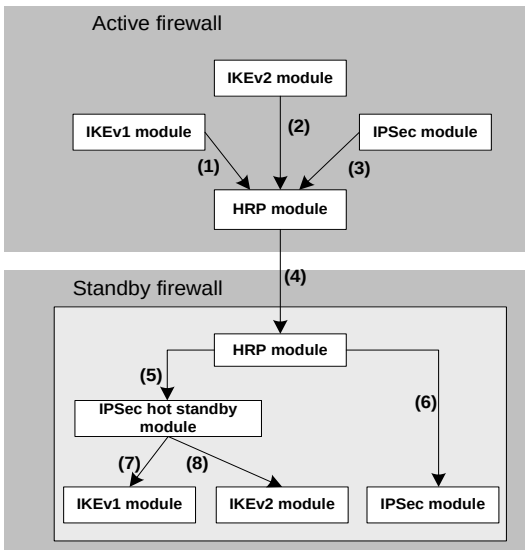


Figure 2-2 shows IPSec hot standby data flows. In the IPSec hot standby system, the active firewall backs up configuration, status, IKE SA, and IPSec SA information to the standby firewall. If the active firewall fails, the standby firewall can process IPSec services.

IPSec hot standby has the following backup modes:

- **Real-time backup:** The objects are backed up to the standby firewall as soon as they are generated. Real-time backup applies to IKE SA and IPSec SA information.
- **Batch backup:** The active firewall backs up all IPSec information to the standby firewall in the case that the standby firewall unexpectedly restarts.
- **Periodic backup:** If all information is synchronized to the standby firewall in real time, the two firewalls are too busy to process these backup packets, causing heartbeat interface congestion, backup packet loss, or heartbeat timeout. Therefore, some information, such as anti-replay sequence numbers, is backed up when the timer expires or the buffer becomes full.

2.5 IPSec Load Balancing

IPSec load balancing enhances IPSec hot standby in terms of reliability and flexibility. IPSec load balancing falls into the following scenarios:

- Dual-tunnel backup
- IPSec load balancing with the Open Shortest Path First(OSPF) protocol
- IPSec load balancing with the Virtual Router Redundancy Protocol (VRRP)

2.6 IPSec Load Balancing Mechanism

1. Dual-tunnel backup

   NGFWs support dual-tunnel applications. A branch can establish tunnels to two hot-standby firewalls that process services at the same time. If one tunnel fails, services traveling through this tunnel immediately switch to the other tunnel. In this mode, IPSec on the two firewalls works independently, and no IPSec information is backed up between the firewalls.

2. IPSec load balancing with OSPF

   OSPF is an internal network gateway protocol based on link status. OSPF routes are advertised to guide traffic and work with IPSec for load balancing. The two firewalls synchronize IPSec information. If one firewall fails, services switch to the other.

3. IPSec load balancing with VRRP

   VRRP is a fault-tolerant protocol applying to local area networks (LANs) that support multicasting and broadcasting. VRRP considers several routers a VRRP group, assigns a virtual IP address and a virtual MAC address to the group, and uses the router with the highest priority in the group as the master router. Only the master router sends and forwards the packets with the virtual IP address as their next hops, and other routers in the group are standby. Services are not interrupted as long as one router in the VRRP group is Master.

   VRRP applies to interfaces on different devices. You can add interfaces on two firewalls to VRRP groups for IPSec load balancing. The two firewalls synchronize IPSec information. If one firewall fails, services switch to the other.

2.7 IPSec QoS Concept

Differentiated services are implemented on the basis of QoS operations, such as traffic classification, traffic policing, traffic shaping, congestion management, and congestion avoidance.

The USG6000 series implements QoS on packets. According to the operation results, the USG6000 series sends the matched packets in an IPSec tunnel. Before encapsulating packets, the USG6000 series classifies the packets and implements QoS on the classified packets to ensure service quality of packets in the IPSec tunnel.

QoS provides the following traffic management technologies:

- **Flow classification**

  Flow classification identifies objects based on matching rules.

- **Traffic policing**

  Traffic policing monitors and manages network traffic. If the traffic exceeds the specified threshold, the USG6000 series keeps the traffic within an appropriate range or takes punitive measures on the excess traffic to protect customers' bandwidths and profits.

- **Traffic shaping**

  Traffic shaping proactively adjusts outgoing traffic of a connection to ensure that the outgoing traffic is sent at an even rate.

- **Congestion management**

  Congestion management defines a scheduling policy for resources to determine the packet forwarding order when a network congestion occurs. Major scheduling policies include queues such as FIFO, CQ, PQ, WFQ, and RTP.

2.8 IPSec QoS Mechanism

Traditional QoS cannot identify packets encapsulated in an IPSec tunnel, and flows cannot be correctly classified. Before encapsulating packets in an IPSec tunnel, IPSec QoS classifies packets to ensure that the packets meet the service quality requirements.

When a packet enters an IPSec tunnel, the USG6000 series checks whether the packet exists in the QoS queue of an interface. If some packets are in the QoS queue, the USG6000 series forwards the packets first. If the QoS queue is full, the USG6000 series discards the excess packet. If no packet is in the QoS queue, the USG6000 series matches the packet with QoS forwarding conditions. If a match is found, the USG6000 series encapsulates and sends the packet. If no matches is found, the packet enters the QoS queue to wait for processing.

2.9 SSL VPN Concept and Mechanism

SSL VPN is an HTTPS-based technology that applies the certificate-based identity authentication, data encryption, and message integrity authentication mechanisms of SSL to secure remote access to intranet resources. SSL VPN has the following advantages:

1. An SSL VPN supports various application protocols. SSL works between the transport and application layers and allows all application programs to share the protection of an SSL VPN.

2. An SSL VPN supports multiple software platforms. Currently, SSL has become a global standard for identifying the website and web browser users and encrypting the communications between browsers and web servers. SSL has been integrated into most browsers, such as Internet Explorer, Netscape, and Firefox. Any computer that runs a common browser supports SSL connections. The SSL VPN client is based on SSL and can be used in most software environments.
3. The SSL VPN gateway supports multiple user authentication methods and refined resource access control to manage remote access to intranet resources.
4. The SSL VPN deployment does not affect the existing network. SSL works at the transport layer and does not change IP packet headers or TCP packet headers Therefore, SSL packets do not require additional NAT configuration. You can enable port 443 for SSL on the USG6000 series, without modifying configurations by application-layer protocol. SSL reduces maintenance efforts and improves security.
5. An SSL VPN supports independent resource access control for domains. Multiple enterprises or departments of an enterprise can share an SSL VPN gateway to reduce deployment costs. Multiple domains can be created on each SSL VPN gateway, and enterprises or departments manage resources and users in their own domains. You can create multiple domains to logically divide an SSL VPN gateway into multiple virtual SSL VPN gateways.

The SSL VPN function of the USG6000 series supports web proxy and network extension.

Web proxy provides HTTP-based web application services for users. When receiving an HTTP request from a user, the USG6000 series works as a web proxy to obtain resources from an intranet web server and returns them to the user.

Network extension installs the virtual network adapter on a client and sets up an SSL VPN tunnel to a gateway to enable and protect access to all IP-based intranet resources.

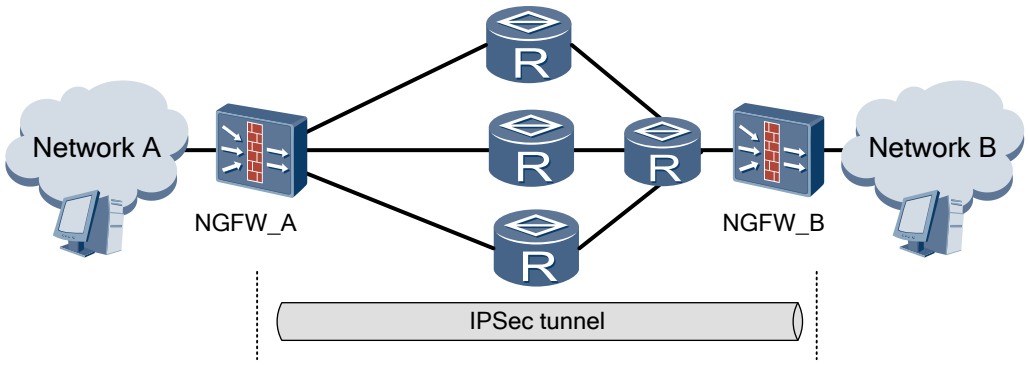
3 Operation and Deployment

This section describes the application scenarios of IPSec.

3.1 Networking Diagram of IPSec Tunneling

Figure 3-1 shows the networking diagram of IPSec tunneling. Network A and network B connect to the Internet respectively through USG_A and USG_B. Multiple links are available for USG_A and USG_B to communicate. If one link is faulty, USG_A and USG_B can communicate over other links. Network A and network B can communicate over an IPSec tunnel.

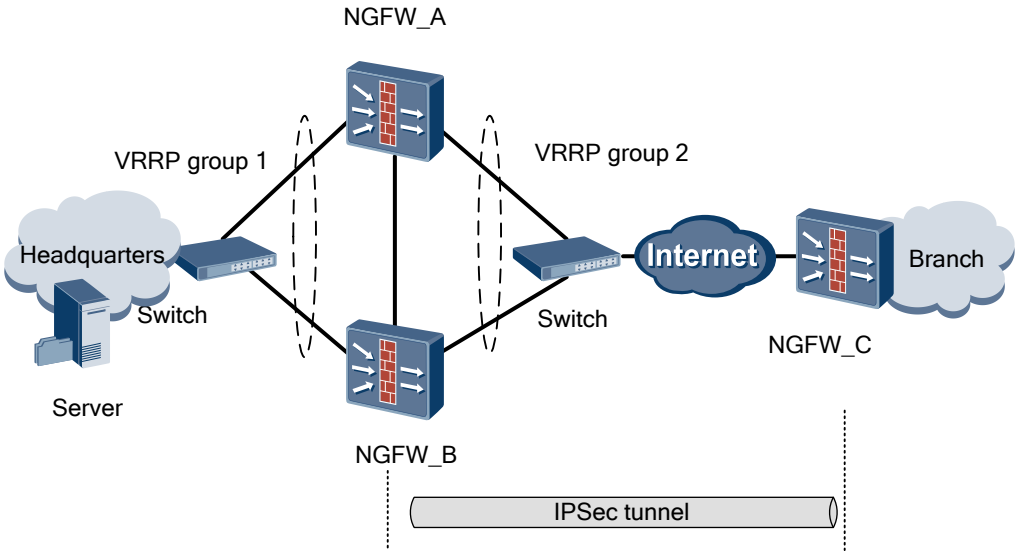
Figure 3-1 Networking diagram of IPSec tunneling



3.2 Networking Diagram of IPSec Hot Standby

Figure 3-2 shows the networking diagram of IPSec hot standby. The server connects to the Internet through the NGFWs. The branch office needs to access the server at the headquarters over an IPSec tunnel. To improve availability, NGFW_A and NGFW_B are configured for active/standby failover. The upstream and downstream devices are switches. NGFW_A can synchronize the IPSec configuration and tunnel information to USB_B to ensure that the IPSec tunnel is available even when NGFW_A is faulty.

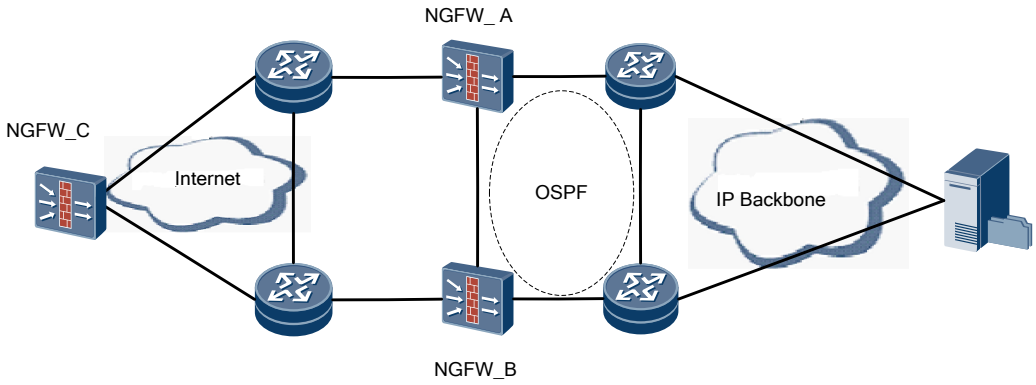
Figure 3-2 Networking diagram of IPSec hot standby



3.3 Networking Diagram of IPSec Load Balancing

Dual-tunnel backup: As shown in Figure 3-3, NGFW_A and NGFW_B, as security gateways, are deployed in front of the backbone network. NGFW_C establishes IPSec VPN tunnels with both NGFW_A and NGFW_B. The IPSec tunnel information on NGFW_A and NGFW_B are not synchronized. The two NGFWs work in load balancing mode to ensure service availability. The upstream and downstream devices are routers. NGFW_A and NGFW_B work together. If one of them is faulty, the other takes over all services.

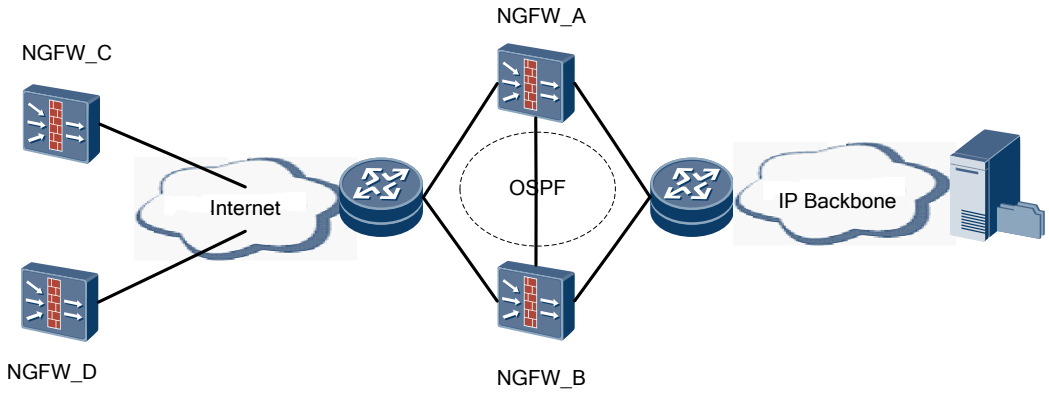
Figure 3-3 Networking diagram of IPSec load balancing in dual-tunnel backup mode



IPSec load balancing (tunnel+OSPF): As shown in Figure 3-4, NGFW_A and NGFW_B, as security gateways, are deployed in front of the backbone network. NGFW_C and NGFW_D at the branch offices establish IPSec VPN tunnels with the headquarters NGFWs to communicate with core network devices. NGFW_A and NGFW_B work in load balancing mode to ensure high availability. The upstream and downstream devices are routers. Service

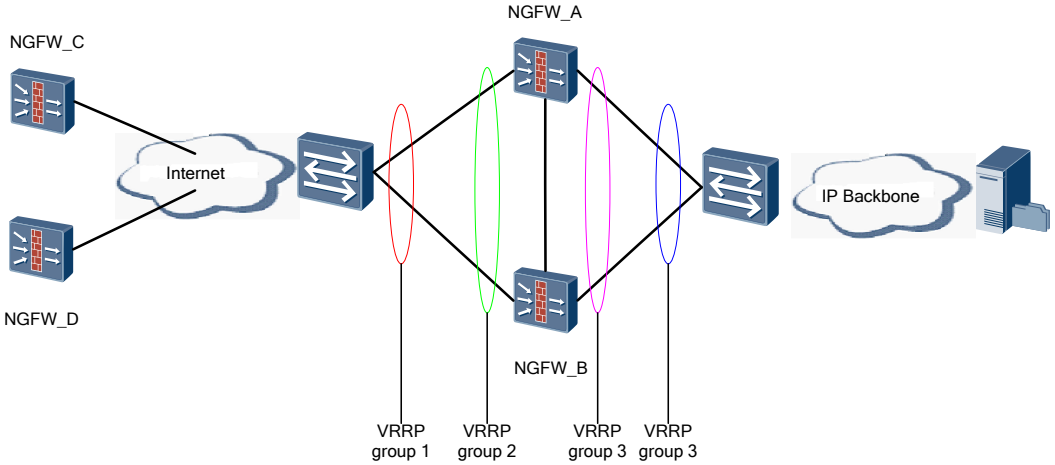
traffic from NGFW_C and NGFW_D is processed respectively by NGFW_A and NGFW_B. If NGFW_A or NGFW_B fails, the other takes over all services.

Figure 3-4 Networking diagram of IPSec load balancing (tunnel+OSPF)



IPSec load balancing with VRRP: As shown in Figure 3-5, NGFW_A and NGFW_B, as security gateways, are deployed in front of the backbone network. NGFW_C and NGFW_D at the branch offices establish IPSec VPN tunnels with the headquarters NGFWs to communicate with core network devices. NGFW_A and NGFW_B work in load balancing mode to ensure high availability. The upstream and downstream devices are switches. Service traffic from NGFW_C and NGFW_D is processed respectively by NGFW_A and NGFW_B. If NGFW_A or NGFW_B fails, the other takes over all services.

Figure 3-5 Networking diagram of IPSec load balancing with VRRP



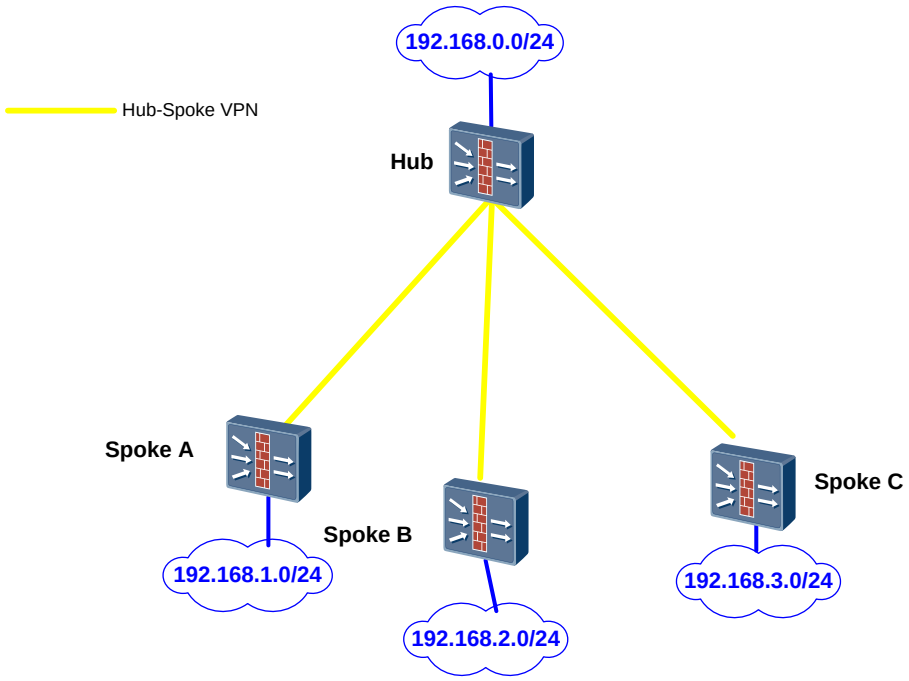
3.4 Networking Diagram of DSVPN

1. Hub-Spoke VPN

In the Hub-Spoke scenario, the Spoke nodes establish VPN tunnels with the Hub node but do not establish tunnels with each other. Traffic between Spoke nodes is relayed by the Hub node.

In this scenario, the tunnel interfaces of the Spoke nodes can be GRE P2P interfaces.

Figure 3-6 Networking diagram of Hub-Spoke VPN

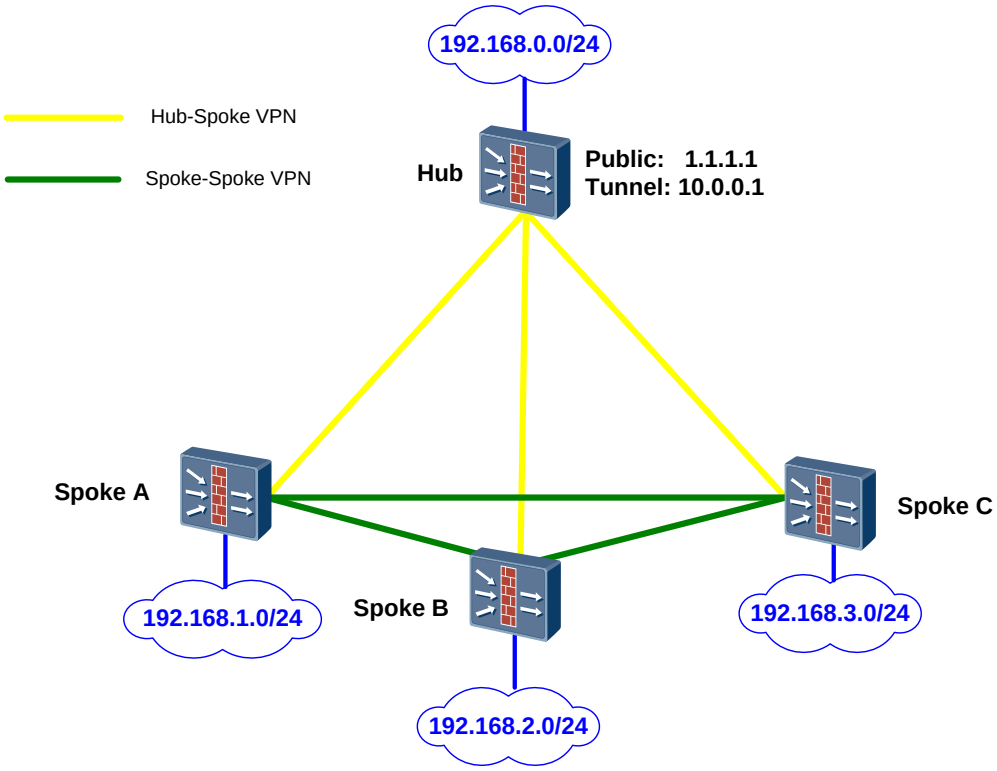


2. Spoke-Spoke VPN

   In the Spoke-Spoke scenario, the Spoke nodes establish VPN tunnels not only with the Hub node but also dynamically with each other based on service requirements.

   In this scenario, all tunnel interfaces must be GRE P2PM interfaces.

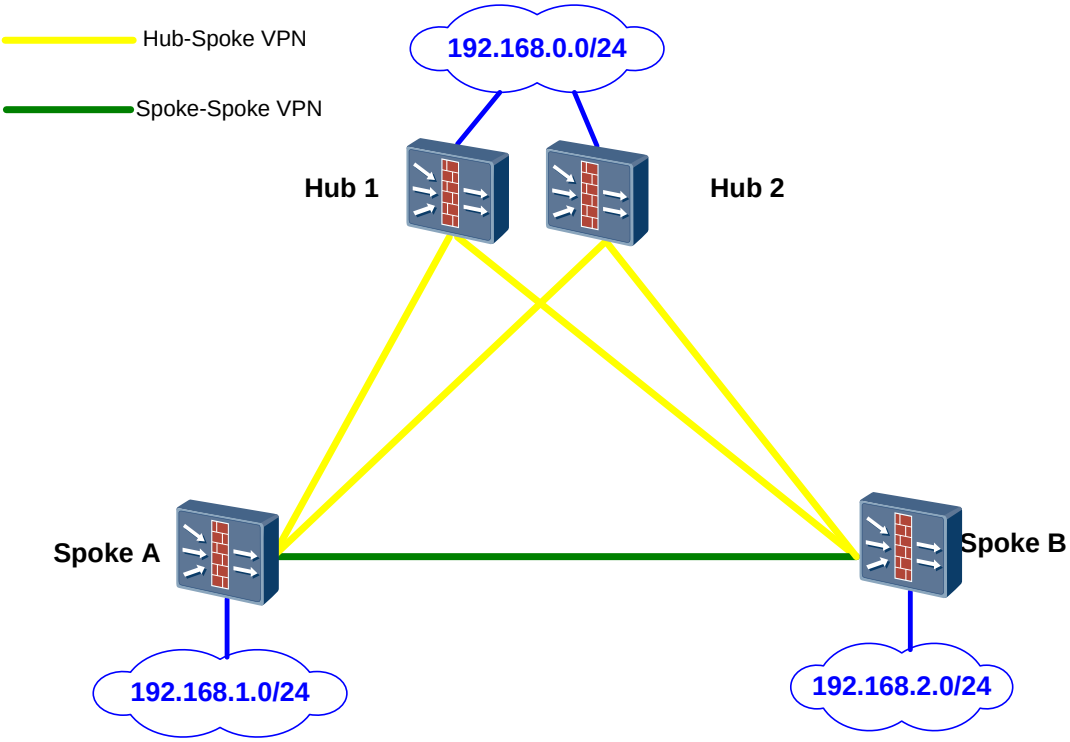
Figure 3-7 Networking diagram of Spoke-Spoke VPN



3. Hub redundancy

   In the Hub redundancy scenario, each Spoke node establishes VPN tunnels with the two Hub nodes. Each Spoke node needs to confirm the active and standby Hub. If the active Hub is Down, the standby Hub takes over.

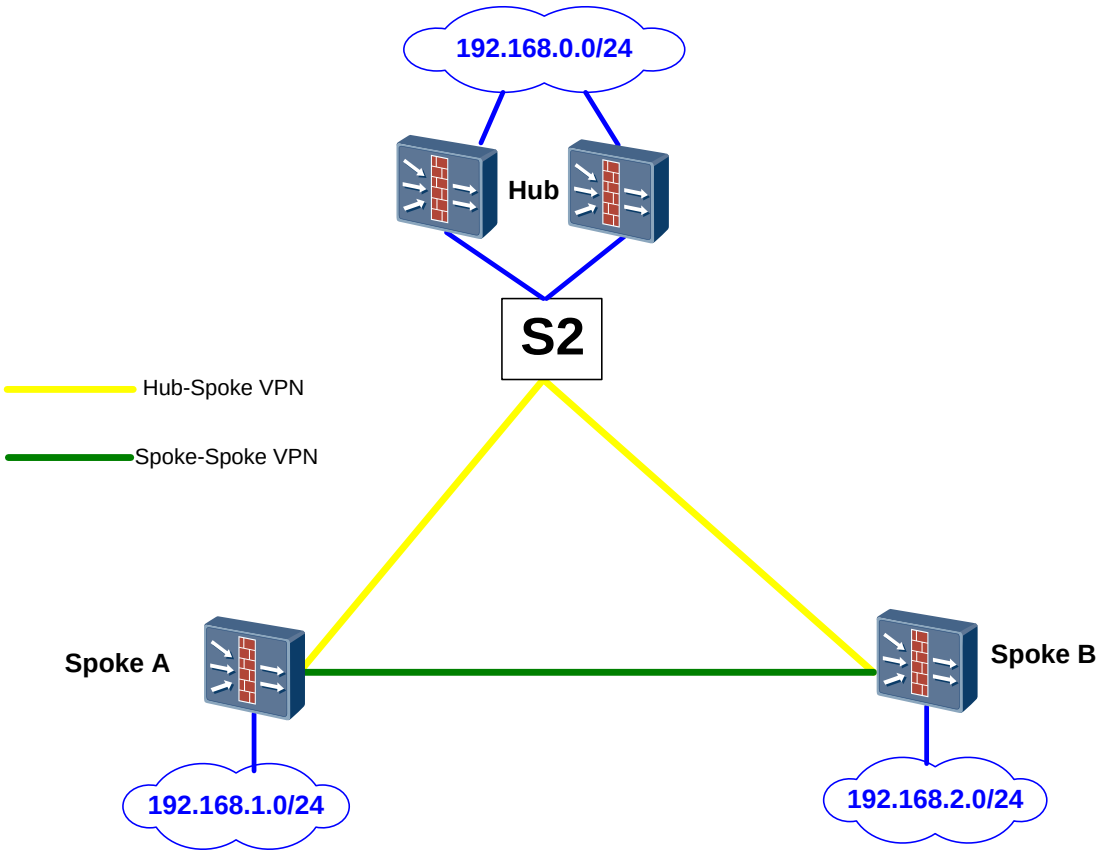
Figure 3-8 Networking diagram of Hub redundancy



4. Hub hot backup

   In the Hub hot backup scenario, the active Hub backs up NHRP entries and IPSec tunnel information to the standby Hub. If the active Hub is Down, the standby Hub takes over.

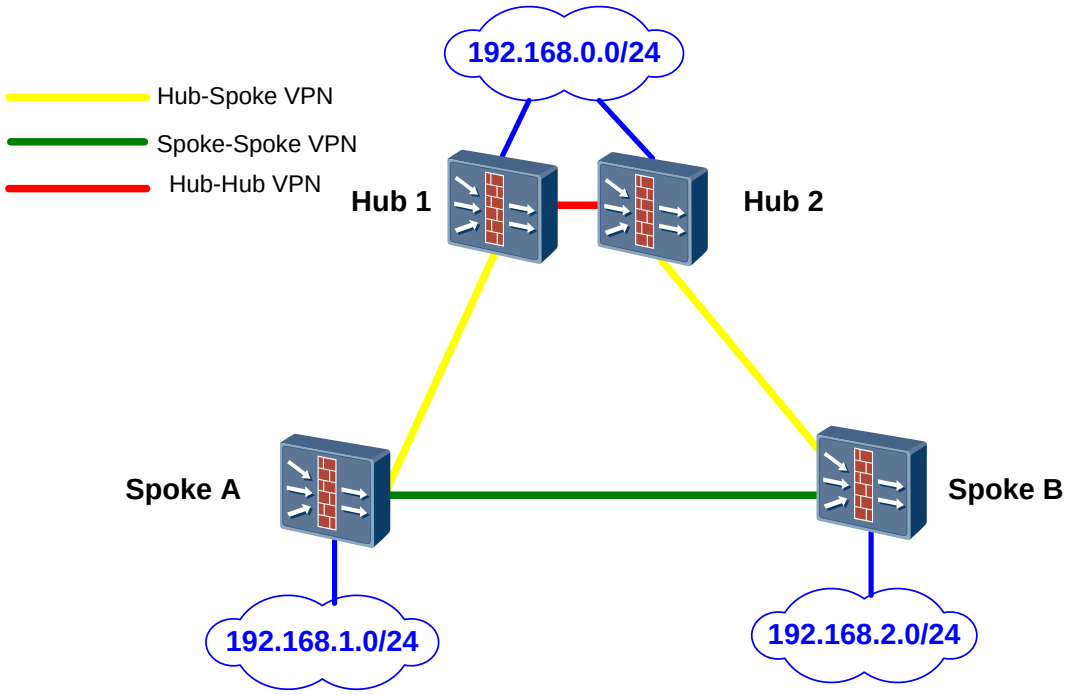
Figure 3-9 Networking diagram of Hub hot backup



5. Hub load balancing

   In the Hub load balancing scenario, the two Hub nodes work together to process services. If one Hub is Down, the other takes over.

Figure 3-10 Networking diagram of Hub load balancing

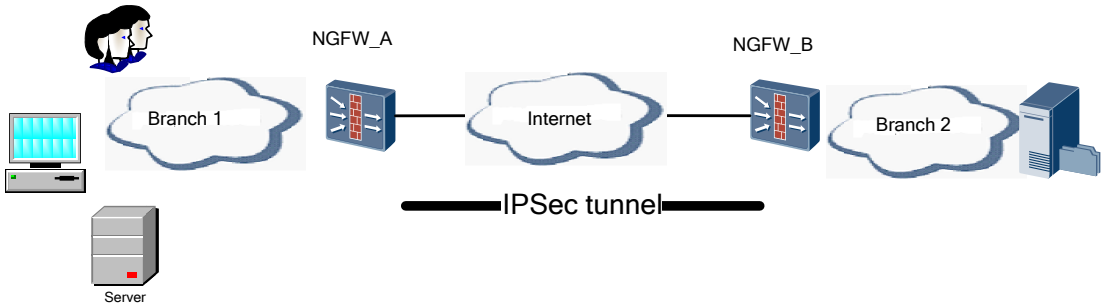


3.5 Networking Diagram of IPSec QoS

1. Bandwidth sharing in one tunnel

   As shown in Figure 3-11, branch offices 1 and 2 of an enterprise locate in different regions. They connect to each other through NGFW_A and NGFW_B. NGFW_A and NGFW_B establish an IPSec tunnel in between. Branch office 1 has multiple types of services, including voice and data services. Due to bandwidth limiting, link congestion may occur during packet transmission. Therefore, configure IPSec QoS to alleviate the congestions and ensure the quality of specific services.

Figure 3-11 Networking diagram of bandwidth sharing in one tunnel

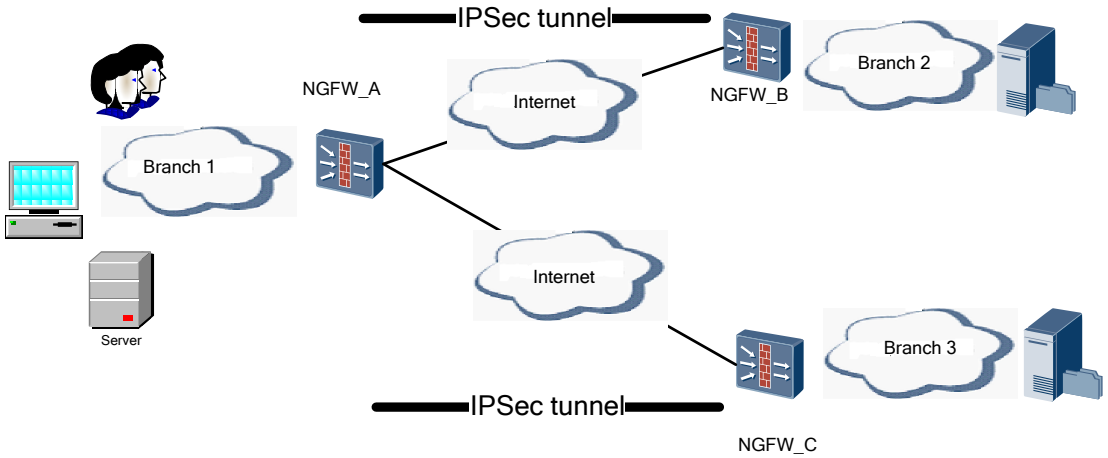


2. Bandwidth sharing by multiple tunnels

   As shown in Figure 3-12, NGFW_A establishes tunnels with NGFW_B and NGFW_C. The two tunnels share one outbound interface on NGFW_A. If the traffic volume in one

tunnel is too large, the interface bandwidth for the other tunnel is decreased. However, the quality of multiple services, such as video and voice services, must be guaranteed. Therefore, apply IPSec QoS on the outbound interface on NGFW_A.

Figure 3-12 Networking diagram of bandwidth sharing by multiple tunnels



3. Bandwidth sharing by IPSec traffic and non-IPSec traffic

   As shown in Figure 3-13, NGFW_A and NGFW_B establish an IPSec tunnel in between to protect only the traffic that matches the specified ACL rules. For branch office 1, only some traffic goes to the IPSec tunnel, and the IPSec traffic and non-IPSec traffic go through the same outbound interface. When the traffic volume is large, IPSec traffic and non-IPSec traffic compete for bandwidths, which may cause packet loss. Therefore, limit the Internet access traffic to guarantee bandwidths for IPSec traffic and ensure the quality of key services.

Figure 3-13 Networking diagram of bandwidth sharing by IPSec traffic and non-IPSec traffic