CHAPTER-1

INTRODUCTION

1.1 Introduction to internship

Internship is the opportunity of integrating the experience by participating in planned and supervised work within an organization for gaining a real time work experience. Only theoretical knowledge of a student is not applicable for working in real world system. Generally, an internship consists of an exchange of services for experience between the student and the organization. Internship helps the students for implementing the theoretical knowledge to the practical aspects for the development of technical and mechanical skills.

Internships are work related learning experiences that provide an opportunity for students, new graduates, and career changes to gain important knowledge and skills in a career related field. An internship is an agreement between student and a company or organization for fixed period of time, such as semester or quarter. Students agree to work for them and they agree to mentor and teach us, internships can offer valuable insight into a particular field or career.

1.2 Objectives of Internship

The report is prepared for the purpose of acquainting the achievement of ours during internship period and the general functions of the company, Digital Outreach Pvt. Ltd. The report has been prepared to accomplish the following objectives:

- To gain knowledge about general work functions in real-world settings.
- To build-vital career-related skills such as organizational, written and interpersonal communication skills.
- To practically implement the knowledge gained from the academics.
- To develop skills and techniques directly applicable to the careers.
- To gain work experience.

1.3 Scope of the Report

The report mainly analyzes the existing services of the company Digital Outreach and the Knowledge that have I have acquired during my internship period. This report mainly includes how technical/network department of Digital Outreach works.

1.4 Methodology

1.4.1 Organization Selection

Since BSc.CSIT program requires enrollment in an organization for a period of ten weeks as an intern, each student needed to select an appropriate organization to join as an intern. As a BSc.CSIT student, I had to select an organization that would be suitable for me. I had choose the networking course during the internship. Among different networking Companies, I found Digital Outreach Pvt. Ltd. To be appropriate as it is the leading enterprise of HUAWEI Company in our country.

1.4.2 Placement

In DOPL, I was provided the opportunity to work as an intern for a period of three months in Baneshwor Kathmandu.

1.4.3 Internship Duration

Start date: 25th September, 2015

Total Duration: 3 months

Supervisor: Mr. Anmol Shrestha (Senior Engineer)

Working Hour: 10:00AM-5:00PM

CHAPTER-2

ORGANIZATIONAL OVERVIEW

2.1 Introduction

Digital Outreach Pvt. Ltd (DOPL) was established with entrepreneurship motive to introduce state-of-the-art solutions for Enterprise and home networking, Surveillance & security and Communication needs of Nepal's growing market through technological development, innovation and transfer. True to its name – DOPL caters to deliver most cost effective digital solutions to business houses in or outside Nepal through own research, innovation and customization. The company offer local solutions to business development and growth through global innovations and technologies. Digital Outreach is the idea, and the spirit of young social entrepreneurs with business acumen to integrate the diverse technological areas catering the need of development through private partnership and services. Today, DOPL is rapidly emerging as a piloting-trading Company, which is sited at New Baneswor, Kathmandu, Nepal.

DOPL seeks to integrate three most important aspect of today's modern society-Networking, Security, and Communication to provide most satisfactory services for our valuable customers through innovative and customized digital solutions.

Our mission is to provide most cost effective solutions for Enterprise and Home Networking and Security System through standard and quality service and support. DOPL is expanding its scope to telecommunication industry to provide effective installation and maintenance services. DOPL priority has always been to server its clients with reliable services and quality products.

2.2 DOPL Services

DOPL is a service oriented company and has been [providing quality services in terms of technical assistance and also providing comprehensive solution on three different aspect of today's modern society. DOPL caters many brands and solutions to meet its customer's unique requirement in its predefined scope.

2.2.1 Enterprise and Home Networking Solutions

DOPL specializes in designing the total business solution for your company. As per the need of the business house, we provide effective networking solutions and PABX networking services and as well as necessary component distribution. In the field of Networking Solutions, DOPL is aggressively working to penetrate the corporate and banking sector of Nepal's market. However, DOPL is also working side by side to provide networking in SOHO market. Previously, DOPL catered various enterprise and networking products from most of the renowned brands such as Cisco, HP, Level One, IBM to name few. With its Value Added Partnership (VAP) with Huawei Technologies Co. Ltd for Enterprise Products in Nepal, DOPL is aggressively working to create a brand image of Huawei Products in today's market. Slow, but effectively, DOPL has been successful in penetrating Huawei products in some renowned corporate houses, government and banking sectors. With

Huawei's vast line of IT and Networking products, DOPL is confident to achieve even more market share for Huawei Enterprise products in near futures.

DOPL also provides effective PBX solution to-medium-to-large business customers as per their requirement. DOPL Technical Teams are more than capable to provide necessary cabling and networking for both analog and IP PBX systems.

Products and Service Portfolio:

- **Enterprise and Home Networking Solutions:** SOHO Routers, Enterprise Routers, SOHO switch, Enterprise Switch (Manageable/Unmanageable), Enterprise Firewall, Media converters.
- **IT Solutions:** Server, Storage, Virtualization, Antivirus.
- **Conferencing Solutions:** Video conference Unified communication, Web Meeting/Conference.
- **PBX Solutions:** Analog PBX and IP PBX.
- **Installation Services:** Complete wiring and installation Required for Networking and PBX solutions
- **Annual Maintenance Services**

2.2.2 Surveillance & Security Services

DOPL specialist teams have an extensive track record in creating tailor-made system to meet the most complex and demanding surveillance & security needs. We combine the right products with the highest standards of consultation, installation and support, to fulfill our client's unique requirements.

Surveillance System (CCTV)

DOLP has been creating skilled teams consisting of engineers and technicians that are fully associated for the installation of CCTV and Internet Protocol (IP) CCTV equipments with highest standards. DOPL specialist teams have an extensive track record in creating in tailor-made system to meet the most complex and demanding security & surveillance needs. DOPL has been providing security and surveillance products from analogue to fully integrated IP system with structured cable networks, cameras, routers and network video recorders, allowing its clients to remotely view and store images over their existing network, or the internet. Currently, DOPL caters surveillance products from bands like Zhejiang Dahua Technology Co. Limited, Huawei , Saitell, LevelOne, Planet to name few.

Product and Service Portfolio:

- **Surveillance:** Analog CCTV, Digital Video Recorder (DVR) IP Camera, Network Video Recorder (NVR).
- **Installation Service:** Complete writing and installation required for CCTV.
- **Annual Maintenance Service.**

2.2.3 Communication Services

DOPL entered the Telecommunication sector from 2010 and since have been developing corporate relationship with the telecommunication Vendors and Service Providers for providing maintenance and installation services. DOPL is working towards complete service solutions required for Telecommunication installation from tower creation to power works to BTS installation and configuration. Currently DOPL is working with Airspan and Nepal Telecom (Nepal's first Mobile Operator) to provide complete installation service for WiMAX service in Nepal.

2.3 DOPL Partners

- Huawei Technologies Co., Pvt.
- Jhejiang Dahua Technology Ltd.
- Neoteric Nepal Pvt. Ltd.
- Silvercrest Networks Pvt. Ltd.

2.4 DOPL Major Clients

DOPL has successfully achieved a high level of customer appreciation, resulting in long lasting relations .Some of our project and clients includes:

Nepal Bank Limited, New Road, Kathmandu	Net Max Technology Pvt. Ltd, Anamnagar
Siddhartha Bank Limited, Kaliya and Manahara Branch,21012	Sagarmatha Merchant Banking and Finance Ltd,Minbhawan,2012
KediaOrganisation,Kamaladi,2011	Music Nepal, Anamnagar, Kathmandu 2011
CA Secretariat Office, Singhadurbar Under the Project Support to Participatory Constitution Building in Nepal (SPCBN), UNDP	Saleways Supermarket Pvt. Ltd Maharajgunj and Pokhara Branch, 2010
Nepal SBI Bank Durbarmarg and Maharajgunj Branch, 2010	District Development Office, Siraha.
Smart Telecom Pvt. Ltd Kumaripati	Ministery of Land, Reform and Management Department of Survey, Minbhawan
Worldlink Pvt. Ltd, Pulchowk	Venus IT Solutions, Kathmandu

CHAPTER 3

REQUIREMENT AND ANALYSIS

3.1 Product Requirement

It describes the position, characteristics, networking and application, functions and features, device structure, maintenance and management, technical specifications, hardware description and features description for the AR and Eudemon.

3.1.1 Secospace USG2110-F-W series

3.1.1.1 Product Overview

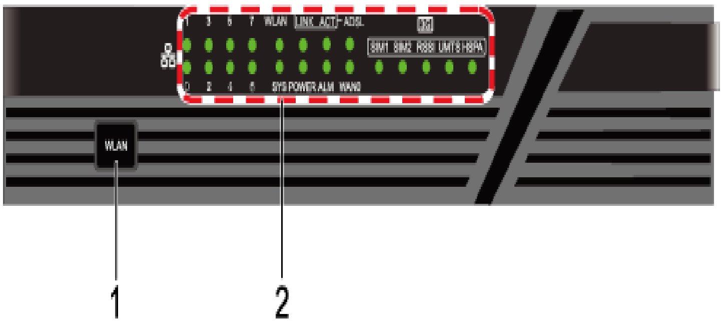
The Secospace USG2110-F-W series of Huawei production integrates security functions including IPS, AV, URL filtering, application control and content filtering and other functions such as routing, switching, VPN, bandwidth management and other networking protection providing a reliable and secure network for different enterprises.

\

Figure 1: Secospace USG2110-F-W series of Huawei

3.1.1.2 Product Appearance

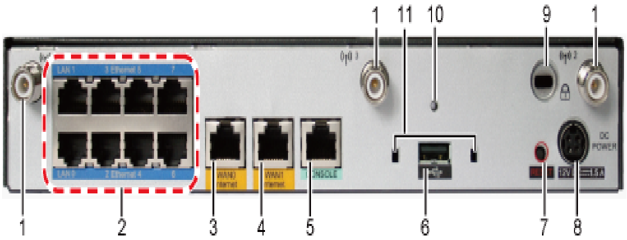
Front Panel



1. WiFi on-off	2. Indicator

Figure 2: Front Panel of Secospace USG2110-F-W series of Huawei

Rear Panel



1. WiFi antenna connectors	2. 10/100M LAN interface
3. WAN0 interface	4. WAN1 interface
5. Console port	6. USB2.0 interface
7. Reset button	8. Power socket
9. Security lock hole	10. USB anti-theft installation hole
11. USB anti-theft locating hole	-

Figure 3: Rear Panel of Secospace USG2110-F-W series of Huawei

3.1.2 Eudemon200E-X1AGW-C

3.1.2.1 Product Overview

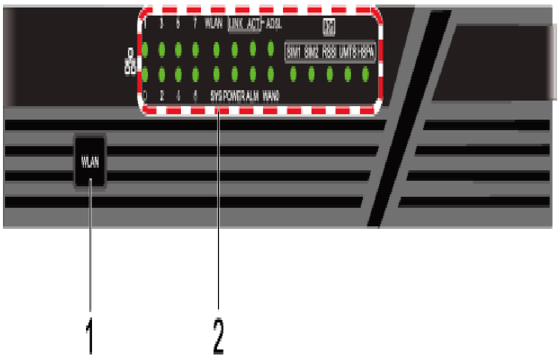
The Eudemon200E-X1AGW-C series is a new-generation product launched by Huawei to meet the requirements of small and medium-sized enterprises, branches of large enterprises, SOHO users, and cyber bars.

Based on the modular design, the Eudemon200E-X1AGW-C series integrates multiple features such as security, routing, switching, and wireless (WiFi and 3G) features. With varieties of interface types and industry-leading performance, the Eudemon200E-X1AGW-C series delivers sound security protection for small and medium-sized enterprises, branches of large enterprises, SOHO users, and cyber bars. In addition, the Eudemon200E-X series provides the integrated network egress security and interworking solution, which helps enterprises decrease cost and increase production efficiency. The Eudemon200E-X1AGW-C series, as a security protection device, is an ideal option for small and medium-sized enterprise networks.

Figure 4: Eudemon200E-X1AGW-C series

3.1.2.2 Product Appearance

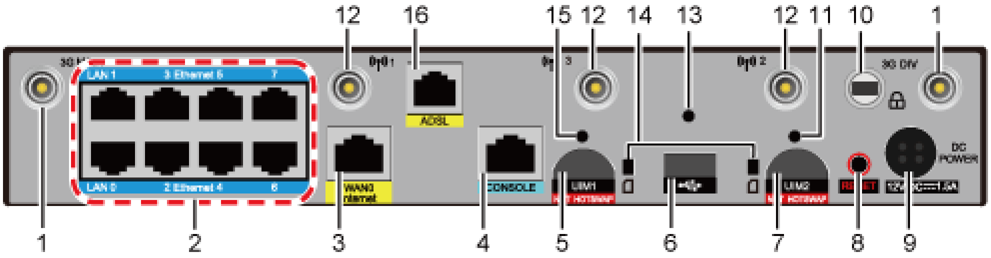
Front Panel



1. WiFi on-off	2. Indicator

Figure 5: Front Panel of Eudemon200E-X1AGW-C series

Rear Panel



1. 3G antenna connectors	2. 10/100M LAN interface	3. WAN0 interface
4. Console port	5. UIM1 slot	6. USB2.0 interface
7. UIM2 slot	8. Reset button	9. Power supply
10.Security lock hole	11.UIM2 anti-theft installation hole	12.WiFi antenna connectors
13.USB anti-theft installation hole	14.USB anti-theft locating hole	15.UIM1 anti-theft installation hole
16.ADSL interface		

Figure 6: Rear Panel of Eudemon200E-X1AGW-C series

CHAPTER 4

DESIGN

4.1 Introduction to Policy Based Route (PBR)

The device supports the IP unicast PBR function. This function provides PBRs for IP unicast packets.

Different from routing based on the destination IP addresses of data packets, IP unicast PBR is a routing mechanism based on user-defined policies. It is used for security and load balancing.

The PBR flexibly controls packet forwarding along different routes based on such information as the ACL rule, user, and application.

In most cases, PBR on an interface is adopted for common forwarding and security.

Currently, the local PBR can be configured only in CLI mode.

When the outbound interface or next hop is specified in the PBR, the route has a higher priority over the common route (by searching the routing table based on the destination IP address of the packet). However, if the default outbound interface or next hop is specified, packets are preferentially forwarded based on the common route. If no match is found, packets are then forwarded based on the PBR.

4.1.1 Policy Based Route

A policy-based route allows packets to be categorized by source IP address, destination IP address, port, user, or application protocol. Packets then can be forwarded using different routes.

4.1.2 Creating a Policy

A policy is used to import routes and select a route for forwarding IP packets.

You can associate multiple policies to a device. A policy consists of policy nodes, each having matching items and operation items.

- Each policy node is identified by a unique node number. A smaller node number indicates a higher priority, and the node with higher priority is executed preferentially.
- The matching items are the ACL, user/user group, and application protocol. Packets are categorized by these matching items. There is an AND relationship among the matching items. Specifically, if a policy node has multiple items to match, only the packets that match all these items are allowed through.
- The operation items require you to specify the outbound interface and next hop for packet forwarding. The packets that meet the matching items are forwarded according to the settings of operation items, namely, are forwarded through the outbound interface specified by the operation items. When a policy node is controlled by the two operation

items, the outbound interface is prior to the next hop. Packets are forwarded to the outbound interface, and to the next hop only when the outbound interface is in Down state.

- The actions that each policy node performs on packets are Deny or Permit.

4.1.3 Network Requirements

As shown in Figure 7 , you need to configure the PBR to ensure that the following requirements are met on USG_A.

- All packets received through GigabitEthernet 0/0/3 from 192.168.1.0/24 are sent to next-hop 1.1.2.2.
- All packets received through GigabitEthernet 0/0/1 from 192.168.0.0/24 are sent to next-hop 1.1.3.2

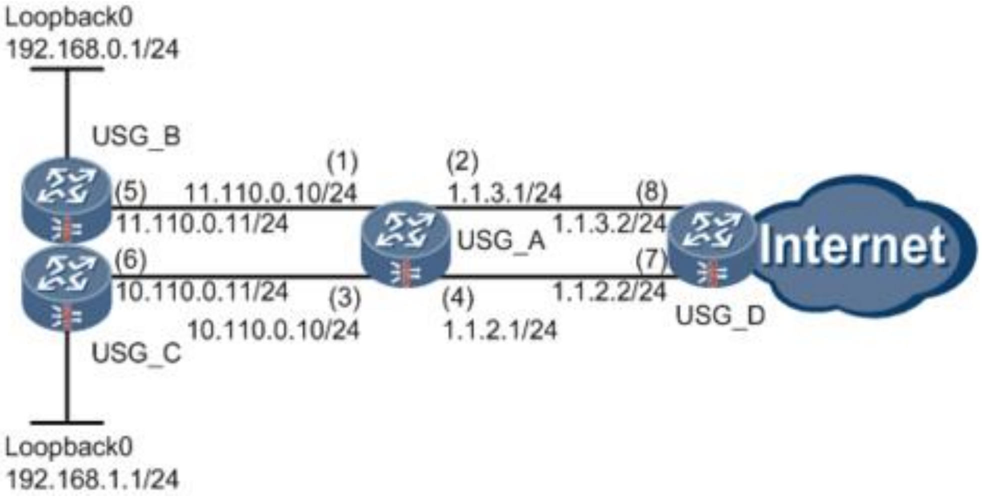
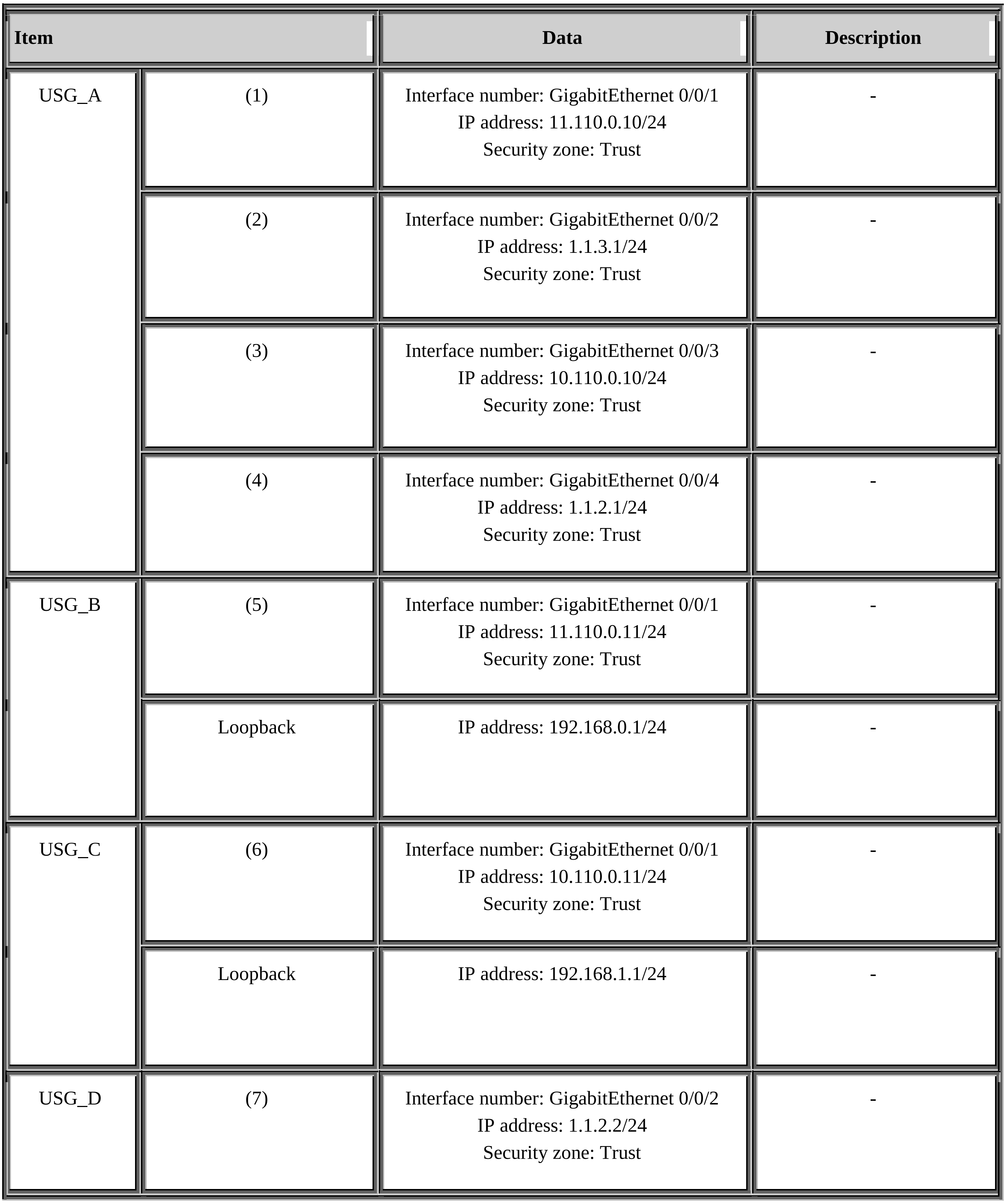


Figure 7: Networking diagram of configuring the PBR based on the source IP address



Item		Data	Description
USG_A	(1)	Interface number: GigabitEthernet 0/0/1 IP address: 11.110.0.10/24 Security zone: Trust	-
	(2)	Interface number: GigabitEthernet 0/0/2 IP address: 1.1.3.1/24 Security zone: Trust	-
	(3)	Interface number: GigabitEthernet 0/0/3 IP address: 10.110.0.10/24 Security zone: Trust	-
	(4)	Interface number: GigabitEthernet 0/0/4 IP address: 1.1.2.1/24 Security zone: Trust	-
USG_B	(5)	Interface number: GigabitEthernet 0/0/1 IP address: 11.110.0.11/24 Security zone: Trust	-
	Loopback	IP address: 192.168.0.1/24	-
USG_C	(6)	Interface number: GigabitEthernet 0/0/1 IP address: 10.110.0.11/24 Security zone: Trust	-
	Loopback	IP address: 192.168.1.1/24	-
USG_D	(7)	Interface number: GigabitEthernet 0/0/2 IP address: 1.1.2.2/24 Security zone: Trust	-

	(8)	Interface number: GigabitEthernet 0/0/3 IP address: 1.1.3.2/24 Security zone: Trust	-

4.2 Overview of IPSec

4.2.1 IPSec SA

The IPSec Security Association (SA) refers to the tunnel parameter agreement made by communications parties who need to establish the IPSec tunnel. The parameters include the IP addresses of the two ends of the tunnel, authentication mode, authentication algorithm, authentication key, encryption algorithm, authentication key, shared key, and duration.

4.2.2 Introduction to SA

The endpoints that communicate with the IPSec are called the IPSec peer.

To establish the IPSec tunnel, the IPSec peers need to negotiate the tunnel parameters. The SA refers to the tunnel parameter agreement made by communications parties who need to establish the IPSec tunnel. The parameters include the IP addresses of the two ends of the tunnel, authentication mode, authentication algorithm, authentication key, encryption algorithm, authentication key, shared key, and duration.

The SA is unidirectional (inbound direction or outbound direction). The bi-directional communication between two peers needs at least two SAs to protect the data flow of the two directions respectively. As shown in Figure 8 , to establish an IPSec tunnel between USG_A and USG_B, two SAs need to be established. SA 1 defines the protection mode of the data from USG_A to USG_B. SA 2 defines the protection mode of the data from USG_B to USG_A. SA 1 is outbound to USG_A, and is inbound to USG_B. Directions of SA 2 are opposite to those of SA 1.

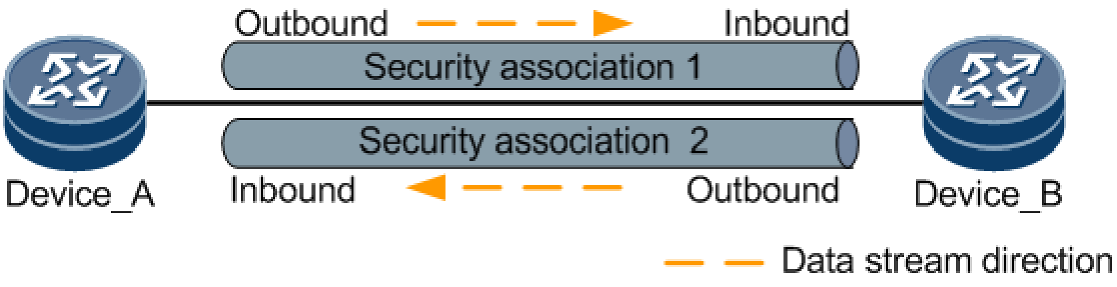


Figure 8: IPSec SA

4.2.3 SA Establishment Modes

On the USG, there are two modes to establish the SA.

- Manual mode.

The advantage of the manual mode is to realize the IPSec function without the IKE. The disadvantage lies in that all information needed to create the SA must be configured manually. The configuration is complicated and some features are not supported.

- IKE negotiation mode.

  The IKE negotiation mode is simpler. You only need to configure the IKE negotiation IPSec policy. The IKE automatically negotiates to create and maintain the SA.

When the peer devices that communicate with the USG are of a smaller number or the environment is statistic and small, you can choose the manual mode for SA establishment. In the medium-sized or large dynamic network environment, it is recommended to use the IKE automatic negotiation mode to establish the SA.

4.2.7 Point to Point IPSec Tunnel

Network Requirements

Network A and network B are connected to the Internet through USG_A and USG_B. An IPSec tunnel is established between USG_A and USG_B to protect the communication security of the two networks, as shown in Figure 9 . The network environment is as follows:

- Network A belongs to subnet 10.1.1.0/24, and is connected to USG_A through interface GigabitEthernet 0/0/1.
- Network B belongs to subnet 10.1.2.0/24, and is connected to USG_B through interface GigabitEthernet 0/0/1.
- USG_A and USG_B are reachable.

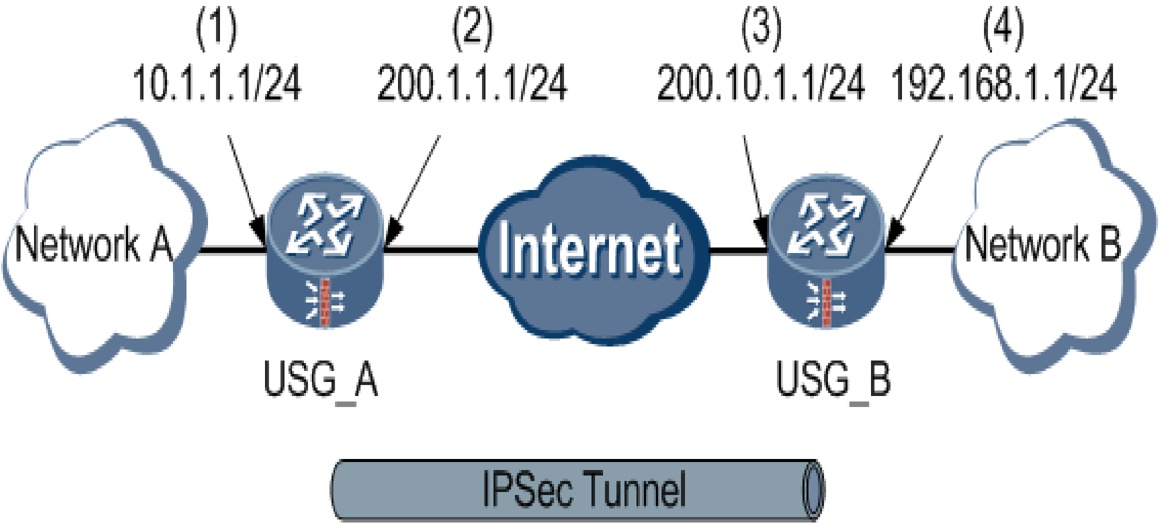


Figure 9: Networking diagram for a point-to-point IPSec tunnel in IKE negotiation mode

Item		Data
USG_A	(1)	Interface number: GigabitEthernet 0/0/1 IP address: 10.1.1.1/24 Zone: Trust
	(2)	Interface number: GigabitEthernet 0/0/2 IP address: 200.1.1.1/24 Zone: Untrust
	IPSec configuration	Local ID type of IKE: IP IKE pre-shared key: abcde IKE peer address: fixed IP address, 200.10.1.1
USG_B	(3)	Interface number: GigabitEthernet 0/0/2 IP address: 200.10.1.1/24 Zone: Untrust
	(4)	Interface number: GigabitEthernet 0/0/1 IP address: 192.168.1.1/24 Zone: Trust
	IPSec configuration	Local ID type of IKE: IP IKE pre-shared key: abcde IKE peer address: fixed IP address, 200.1.1.1

4.3 Overview of GRE

General Routing Encapsulation (GRE) indicates the encapsulation of the packets of certain network layer protocols, such as IP. After the encapsulation, these packets can be transmitted according to another network layer protocol, such as IP. GRE provides two security mechanisms: checksum authentication and key authentication.

The transmission of packets in GRE tunnels can be divided into two processes: encapsulation and decapsulation. Take the network shown in Figure 10 as an example.

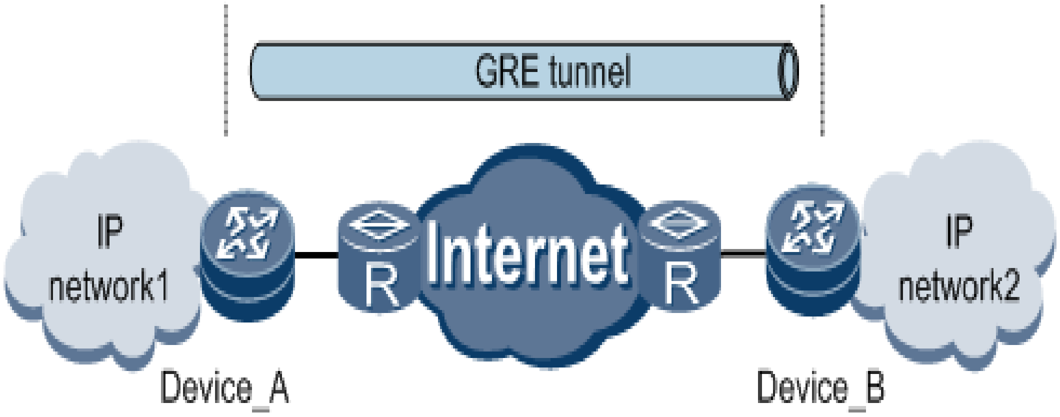


Figure 10: IP network interconnection through the GRE tunnel

- Encapsulation

  After receiving an IP packet, the interface of Device_A that connects to IP network1 submits the packet to the IP protocol module. The IP protocol module checks the destination address in the IP packet header to determine how to forward this packet. If the destination address of the packet is a virtual network address that passes through a tunnel interface, the packet will be forwarded to the tunnel interface. After receiving the packet, the tunnel interface encapsulates the packet with GRE and then submits the packet to the IP protocol module. After encapsulating a new IP packet header, the IP protocol module searches the routing table according to the destination address and then submits the packet to the corresponding interface for processing.

- Decapsulation

  Decapsulation is the reverse of the encapsulation. After the interface of Device_B that connects to the Internet receives an IP packet, the destination address is checked. If the destination address is the IP address of Device_B and the value of the protocol field is 47, the protocol is GRE. In this case, the IP header of the packet is discarded and then the packet is submitted to the GRE protocol module for the check of items such as keywords and checksum. After processing the packet, the GRE protocol module discards the GRE header and submits the packet to the IP protocol module. Then the IP protocol module forwards the packet to IP network2.

4.3.1 GRE Tunnel with Static Route

If the devices on the Internet do not support the transmission of certain data transmitted by intranet devices, you can configure the GRE tunnel for transmission. When a small number of devices exist on the intranet and the IP addresses are fixed, you can configure the static route to transmit the packets sent by the user through the tunnel.

4.3.2 Network Requirements

As shown in Figure 11 , network A and network B connect to the Internet through USG_A and USG_B.

The network environment is as follows:

- The routes to USG_A and USG_B are reachable.
- The USG_A and USG_B use Layer-3 GRE protocol to achieve the interconnection between network A and network B.
- Specify USG_A and USG_B as the default gateways of PC1 and PC2 respectively. Configure static routes between USG_A and PC1, and USG_B and PC2.

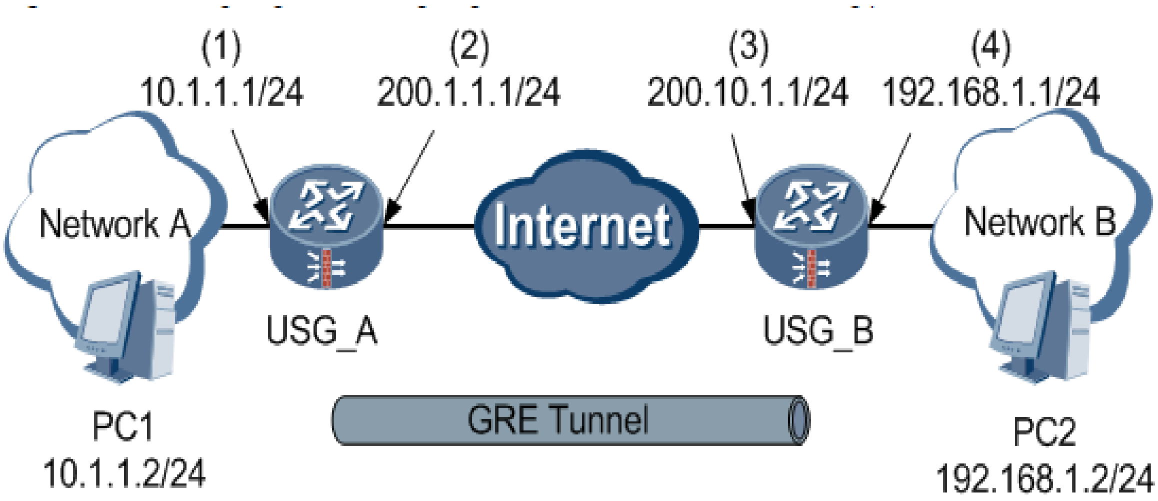


Figure 11: Networking diagram of configuring the GRE tunnel with static routing protocols

Item		Data	Description
USG_A	(1)	Interface number: GigabitEthernet 0/0/1 IP address: 10.1.1.1/24 Zone: Trust	-
	(2)	Interface number: GigabitEthernet 0/0/2 IP address: 200.1.1.1/24 Zone: Untrust	-
	GRE configuration	Interface Name: Tunnel IP address: 40.1.1.1/24 Source IP Address: 200.1.1.1 Destination Address: 200.10.1.1	The IP address of the GRE tunnel interface can be set to an arbitrary value. The IP addresses of interfaces on both ends of the GRE tunnel must be in the same network segment.
USG_B	(3)	Interface number: GigabitEthernet 0/0/2 IP address: 200.10.1.1/24 Zone: Untrust	-
	(4)	Interface number: GigabitEthernet 0/0/1 IP address: 192.168.1.1/24 Zone: Trust	-
	GRE configuration	Interface Name: Tunnel IP address: 40.1.1.2/24 Source IP Address: 200.10.1.1 Destination Address: 200.1.1.1	The IP address of the GRE tunnel interface can be set to an arbitrary value. The IP addresses of interfaces on both ends of the GRE tunnel must be in the same network segment.

4.4 GRE-over-IPSec Tunnel

When data (for example, multicast data) transferred between two devices cannot be directly encapsulated in IPSec, it can first be encapsulated in GRE and then in IPSec.

Network Requirements

As shown in Figure 12 , network A and network B are connected to the Internet through USG_A and USG_B. A GRE-over-IPSec tunnel is established between USG_A and USG_B.

The networking requirements are as follows:

- Network A belongs to subnet 10.1.1.0/24, and is connected to USG_A through interface GigabitEthernet 0/0/1.
- Network B belongs to subnet 192.168.1.0/24, and is connected to USG_B through interface GigabitEthernet 0/0/1.
- USG_A and USG_B are reachable.

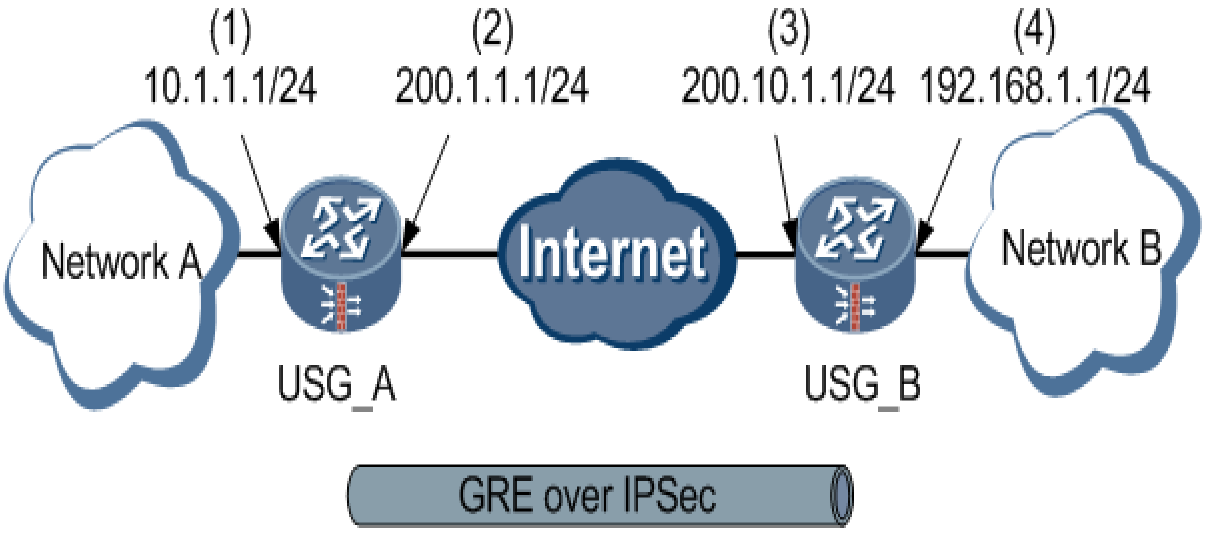


Figure 12: Networking diagram of configuring GRE over IPSec

Item		Data
USG_A	(1)	Interface number: GigabitEthernet 0/0/1 IP address: 10.1.1.1/24 Zone: Trust

Item		Data
	(2)	Interface number: GigabitEthernet 0/0/2 IP address: 200.1.1.1/24 Zone: Untrust
	GRE configuration	Interface name: Tunnel IP address: 40.1.1.1/24 Source IP address: 200.1.1.1 Destination Address: 200.10.1.1
	IPSec configuration	IKE version: V1 and V2 IKE negotiation mode: main mode Local ID type of IKE: IP IKE pre-shared key: abcde IKE peer address: fixed IP address, 200.10.1.1 IPSec encapsulation mode: Tunnel mode IPSec security protocol: ESP
USG_B	(3)	Interface number: GigabitEthernet 0/0/2 IP address: 200.10.1.1/24 Zone: Untrust
	(4)	Interface number: GigabitEthernet 0/0/1 IP address: 192.168.1.1/24 Zone: Trust
	GRE configuration	Interface name: Tunnel IP address: 40.1.1.2/24 Source IP address: 200.10.1.1 Destination Address: 200.1.1.1
	IPSec configuration	IKE version: V1 and V2 IKE negotiation mode: main mode Local ID type of IKE: IP IKE pre-shared key: abcde IKE peer address: fixed IP address, 200.1.1.1 IPSec encapsulation mode: Tunnel mode IPSec security protocol: ESP

CHAPTER 5

IMPLEMENTATION AND TESTING

5.1 Implementation of Source IP Address-Based PBR

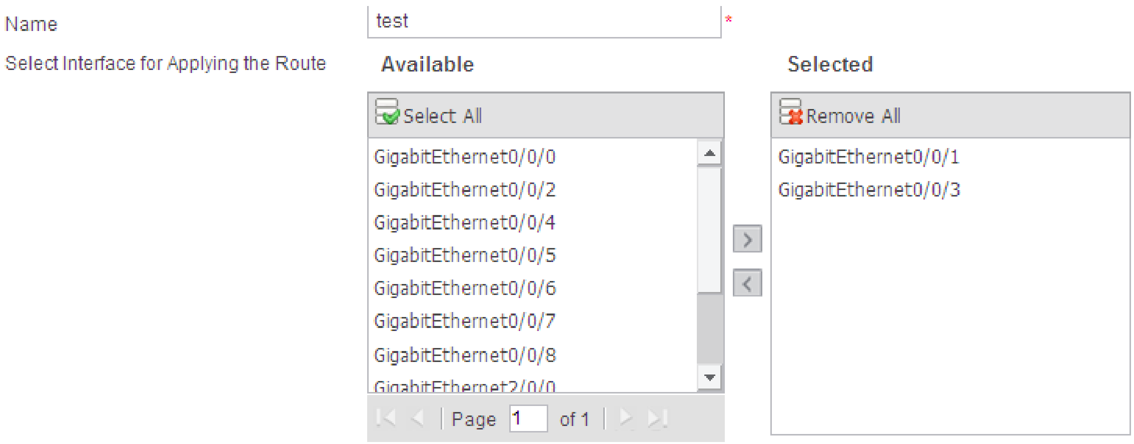
5.1.2 Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the basic parameters of the interfaces.
2. Configure interzone packet filtering to ensure normal communication.
3. Configure the PBR based on the ACL rule. The source IP address defined in the ACL rule is 192.168.1.0/24. The packets matching the ACL rule are forwarded to next-hop address 1.1.2.2 and the PBR is applied to interface GigabitEthernet 0/0/3.
4. Configure the PBR based on the ACL rule. The source IP address defined in the ACL rule is 192.168.0.0/24. The packets matching the ACL rule are forwarded to next-hop address 1.1.3.2 and the PBR is applied to interface GigabitEthernet 0/0/1.

5.1.3 Procedure

1. Configure the basic parameters of the interfaces on USG_A, USG_B, USG_C and USG_D. Details are omitted.
2. For the USG, configure interzone packet filtering to ensure normal network communication. For the USG BSR/HSR, this operation is not required. The following uses the information displayed on USG_A as an example.
    a. Choose **Firewall** > **Security Policy** > **Local Policy**.
    b. Click ✎ in the row where **Implicit** resides in **trust**.
    c. Set **Action** to **permit**.
    d. Click **Apply**.
3. Configure USG_A.
    a. Create policy **test** and apply it to interfaces GigabitEthernet 0/0/1 and GigabitEthernet 0/0/3.
        1. Choose **Router** > **Policy-based Route** > **Policy-based Route**.
        2. Click **Add**.
        3. Enter or select parameters listed in Figure 13.
        4. Click **Apply**.



Name: test *

Select Interface for Applying the Route

Available:
- Select All
- GigabitEthernet0/0/0
- GigabitEthernet0/0/2
- GigabitEthernet0/0/4
- GigabitEthernet0/0/5
- GigabitEthernet0/0/6
- GigabitEthernet0/0/7
- GigabitEthernet0/0/8
- GigabitEthernet2/0/0

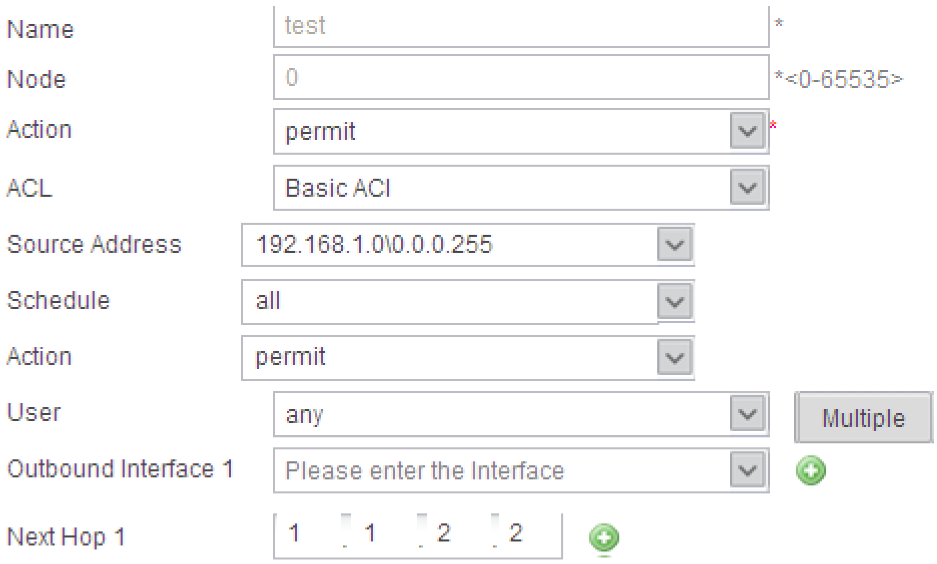
Page 1 of 1

Selected:
- Remove All
- GigabitEthernet0/0/1
- GigabitEthernet0/0/3

Figure 13: Creating policy **test**

b. Modify policy node **0** to match IP packets by using the ACL rule, so that packets at 192.168.1.0/24 can be forwarded to next-hop address 1.1.2.2.

1. In **Policy-based Route List**, click ✎ in the row where node **0** resides in **Policy Name : test**.
2. Enter or select parameters listed in Figure 14.
3. Click **Apply**.

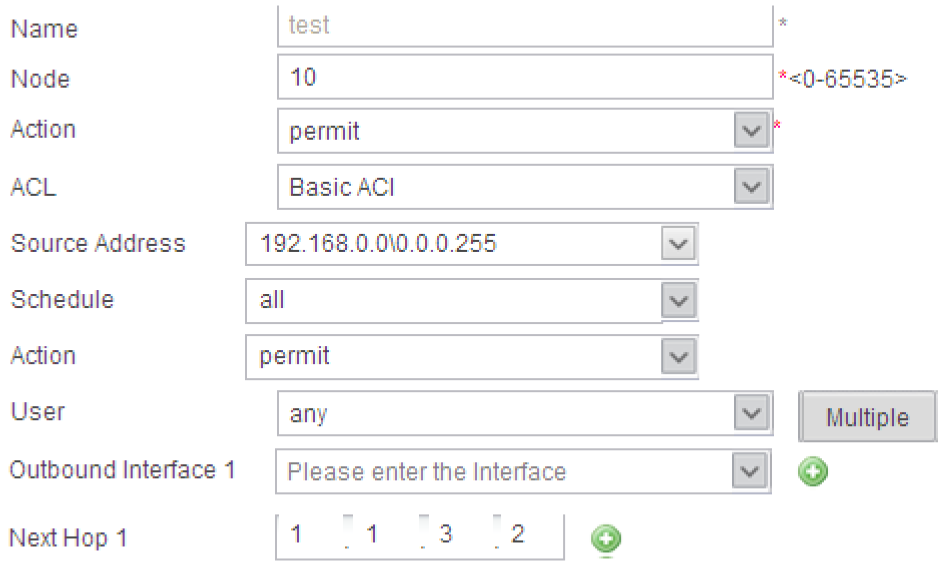


Name	test *
Node	0 *<0-65535>
Action	permit *
ACL	Basic ACl
Source Address	192.168.1.0\0.0.0.255
Schedule	all
Action	permit
User	any
Outbound Interface 1	Please enter the Interface
Next Hop 1	1 . 1 . 2 . 2

Figure 14: Modifying policy node **0**

c. Modify policy node **10** to match IP packets by using the ACL rule, so that packets at 192.168.0.0/24 can be forwarded to next-hop address 1.1.3.2.

1. In **Policy-based Route List**, click ✚ of **Policy Name : test**.
2. Enter or select parameters listed in Figure 15 .
3. Click **Apply**.



Name	test *
Node	10 *<0-65535>
Action	permit *
ACL	Basic ACl
Source Address	192.168.0.0\0.0.0.255
Schedule	all
Action	permit
User	any
Outbound Interface 1	Please enter the Interface
Next Hop 1	1 . 1 . 3 . 2

Figure 15: Creating policy node **10**

d. Configure a static route from USG_A to 192.168.1.0/24.

1. Choose **Router** > **Static** > **Static Route**.
2. Click **Add**.
3. Enter or select parameters listed in the following:
    1. Destination Address: 192.168.1.1
    2. Mask: 255.255.255.0
    3. Next Hop: 10.110.0.11

    Keep default values for other parameters.
4. Click **Apply**.

e. Configure a static route from USG_A to 192.168.0.0/24.

1. In **Static Route List** click **Add**.
2. Enter or select parameters listed in the following:
    1. Destination Address: 192.168.0.1
    2. Mask: 255.255.255.0
    3. Next Hop: 11.110.0.11

    Keep default values for other parameters.
3. Click **Apply**.

4. Configure a default route with next hop address 11.110.0.10 to USG_B.
5. Configure a default route with next-hop address 10.110.0.10 to USG_C.
6. Configure a static route to USG_D:

- Configure a static route with next-hop address 1.1.2.1 from USG_D to 192.168.1.0/24.
- Configure a static route with next-hop address 1.1.2.1 from USG_D to 10.110.0.0/24.
- Configure a static route with next-hop address 1.1.3.1 from USG_D to 192.168.0.0/24.
- Configure a static route with next-hop address 1.1.3.1 from USG_D to 11.110.0.0/24.

5.2 TESTING

5.2.1 Configuration Verification of Source IP Address-Based PBR

1. On USG_C, verify that source IP address 192.168.1.1 can ping 1.1.2.2/24 but cannot ping 1.1.3.2/24.

   # On USG_C, choose **System** > **Maintenance** > **Diagnosis Center** and click the **Ping** tab. Enter **1.1.2.2** in **Host Name or IP Address** and click **Advanced Configuration**. Enter**192.168.1.1** in **Source IP Address** and click **Ping**. The following information is displayed:

   ```
   PING 1.1.2.2: 56  data bytes, press CTRL_C to break
     Reply from 1.1.2.2: bytes=56 Sequence=1 ttl=255 time=10 ms
     Reply from 1.1.2.2: bytes=56 Sequence=2 ttl=255 time=1 ms
     Reply from 1.1.2.2: bytes=56 Sequence=3 ttl=255 time=1 ms
     Reply from 1.1.2.2: bytes=56 Sequence=4 ttl=255 time=10 ms
     Reply from 1.1.2.2: bytes=56 Sequence=5 ttl=255 time=1 ms

   --- 1.1.2.2 ping statistics ---
     5 packet(s) transmitted
     5 packet(s) received
     0.00% packet loss
     round-trip min/avg/max = 1/4/10 ms
   ```

   # On USG_C, choose **System** > **Maintenance** > **Diagnosis Center** and click the **Ping** tab. Enter **1.1.3.2** in **Host Name or IP Address** and click **Advanced Configuration**. Enter**192.168.1.1** in **Source IP Address** and click **Ping**. The following information is displayed:

   ```
   PING 1.1.3.2: 56  data bytes, press CTRL_C to break
     Request time out
     Request time out
     Request time out
     Request time out
     Request time out

   --- 1.1.3.2 ping statistics ---
     5 packet(s) transmitted
     0 packet(s) received
     100.00% packet loss
   ```

2. On USG_B, verify that source IP address 192.168.0.1 can ping 1.1.3.2/24 but cannot ping 1.1.2.2/24.

   # On USG_B, choose **System** > **Maintenance** > **Diagnosis Center** and click the **Ping** tab. Enter **1.1.3.2** in **Host Name or IP Address** and click **Advanced Configuration**. Enter**192.168.0.1** in **Source IP Address** and click **Ping**. The following information is displayed:

```
 PING 1.1.3.2: 56  data bytes, press CTRL_C to break
   Reply from 1.1.3.2: bytes=56 Sequence=1 ttl=255 time=10 ms
   Reply from 1.1.3.2: bytes=56 Sequence=2 ttl=255 time=1 ms
   Reply from 1.1.3.2: bytes=56 Sequence=3 ttl=255 time=1 ms
   Reply from 1.1.3.2: bytes=56 Sequence=4 ttl=255 time=10 ms
   Reply from 1.1.3.2: bytes=56 Sequence=5 ttl=255 time=1 ms

 --- 1.1.3.2 ping statistics ---
   5 packet(s) transmitted
   5 packet(s) received
   0.00% packet loss
round-trip min/avg/max = 1/4/10 ms
```

   # On USG_B, choose **System** > **Maintenance** > **Diagnosis Center** and click the **Ping** tab. Enter **1.1.2.2** in **Host Name or IP Address** and click **Advanced Configuration**. Enter**192.168.0.1** in **Source IP Address** and click **Ping**. The following information is displayed:

```
 PING 1.1.2.2: 56  data bytes, press CTRL_C to break
   Request time out
   Request time out
   Request time out
   Request time out
   Request time out

 --- 1.1.2.2 ping statistics ---
   5 packet(s) transmitted
   0 packet(s) received
   100.00% packet loss
```

5.3 Implementation of Point to Point IPSec Tunnel

5.3.1 Configuration Roadmap

The public IP addresses of the two networks are fixed and the two networks need to access each other. A point-to-point IPSec tunnel in IKE negotiation mode can be established so that the devices in the two networks can both initiate a connection.

For USG_A and USG_B, the configuration roadmap, is the same and as follows

1. Complete basic interface configurations and route configurations and enable local policy and forwarding policy.
2. Configure the IPSec policy, including basic IPSec policy information, data flow to be protected by IPSec, and proposal parameters for security association negotiation.

5.3.2 Procedure

- Configure USG_A.
    1. Configure the basic parameters of the interfaces.
        a. Choose **Network** > **Interface** > **Interface**.

        b. In **Interface List**, click 📝 of GE0/0/1.

        c. On the **Modify GigabitEthernet Interface** page, configure the following parameters:

        - Zone: trust
        - IP Address: 10.1.1.1
        - Subnet Mask: 255.255.255.0

        Other parameters are set to the default values.

        d. Click **Apply**.

        e. In **Interface List**, click 📝 of GE0/0/2.

        f. On the **Modify GigabitEthernet Interface** page, configure the following parameters:

        - Zone: untrust
        - IP Address: 200.1.1.1
        - Subnet Mask: 255.255.255.0

        Other parameters are set to the default values.

        g. Click **Apply**.
    2. For the USG, configure interzone packet filtering to ensure normal network communication. For the USG BSR/HSR, this operation is not required.

        a. Configure the security policy between the Local zone and the Untrust zone.

        i. Choose **Firewall** > **Security Policy** > **Local Policy**.

ii. In **Local Policy**, click **Add** to configure the following parameters:

- Source Zone: untrust
- Source Address: 200.10.1.0/24
- Action: permit

iii. Click **Apply**.

b. Configure the security policy between the Trust zone and the Untrust zone.

. Choose **Firewall** > **Security Policy** > **Forward Policy**.

i. In **Forward Policy List**, click **Add** to configure the following parameters:

- Source Zone: trust
- Destination Zone: untrust
- Source Address: 10.1.1.0/24
- Destination Address: 192.168.1.0/24
- Action: permit

ii. Click **Apply**.

iii. Choose **Firewall** > **Security Policy** > **Forward Policy**.

iv. In **Forward Policy List**, click **Add** to configure the following parameters:

- Source Zone: untrust
- Destination Zone: trust
- Source Address: 192.168.1.0/24
- Destination Address: 10.1.1.0/24
- Action: permit

v. Click **Apply**.

3. Configure a static route from USG_A to network B, with the next-hop IP address of 200.1.1.2.

a. Choose **Route** > **Static** > **Static Route**.

b. In **Static Route List**, click **Add**.

c. On the **Add Static Route** page, configure the following parameters:

- Destination Address: 192.168.1.0
- Mask: 255.255.255.0
- Next Hop: 200.1.1.2

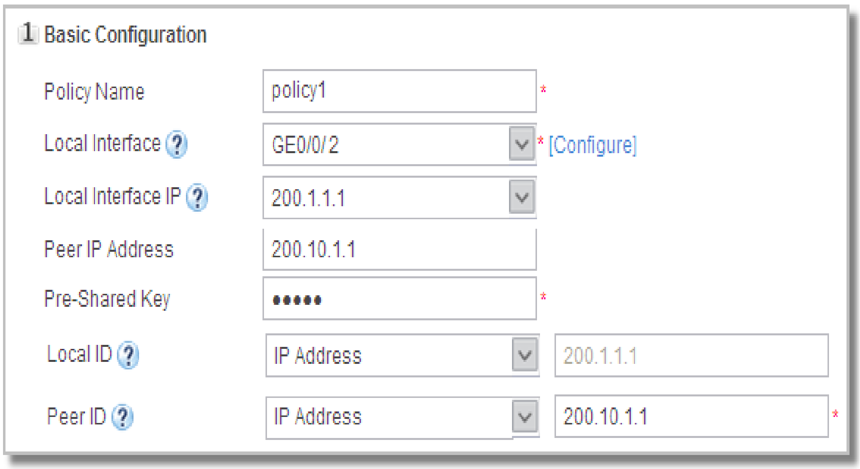
Other parameters are set to the default values.

d. Click **Apply**.

4. Configure the IPSec tunnel on USG_A.

   a. Choose **VPN** > **IPSec** > **IPSec**, click **Add**, and set **Scenario** to **Site-to-site**.

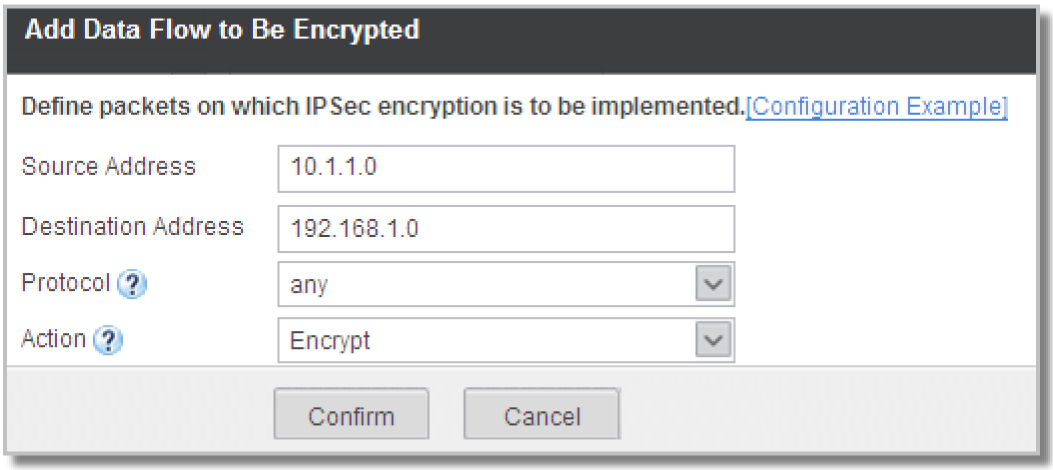
Configure the basic IPSec policy information, specify the remote gateway, and set the pre-shared key to abcde.



1 Basic Configuration

Policy Name	policy1 *	
Local Interface	GE0/0/2 * [Configure]	
Local Interface IP	200.1.1.1	
Peer IP Address	200.10.1.1	
Pre-Shared Key	●●●●● *	
Local ID	IP Address	200.1.1.1
Peer ID	IP Address	200.10.1.1 *

   b. Under **Data Flow to Be Encrypted**, click **Add** to add a data flow as follows.



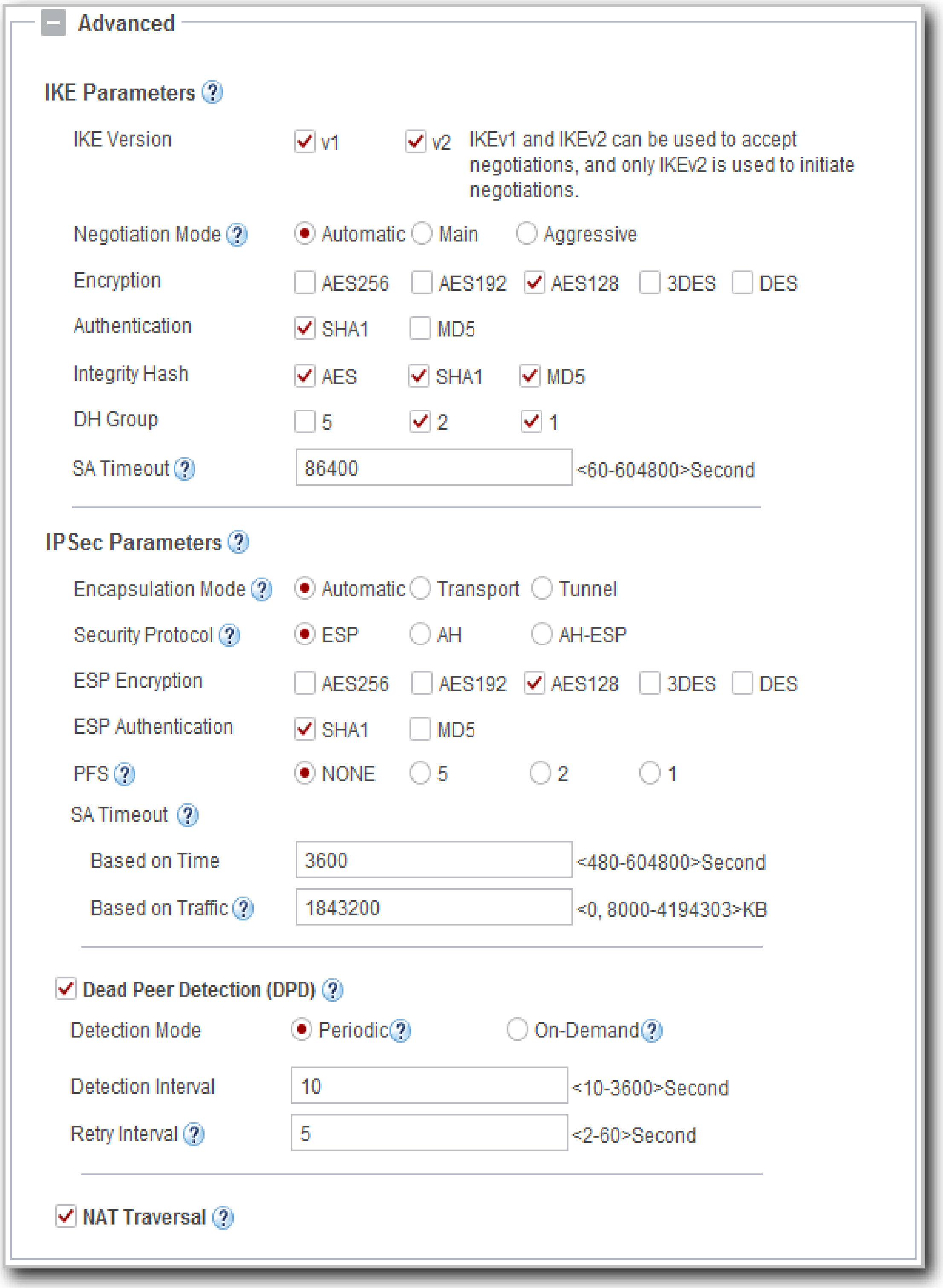
Add Data Flow to Be Encrypted

Define packets on which IPSec encryption is to be implemented.[Configuration Example]

Source Address	10.1.1.0
Destination Address	192.168.1.0
Protocol	any
Action	Encrypt

   c. Under **IKE/IPSec Proposal**, expand **Advanced**, and configure IPSec proposal as follows.

   In this example, all proposal parameters are set to default values, as shown in the following figure. If you change the value of a parameter, you must ensure that the parameter settings are the same on both tunnel ends.



Advanced

IKE Parameters

IKE Version ☑ v1 ☑ v2 IKEv1 and IKEv2 can be used to accept negotiations, and only IKEv2 is used to initiate negotiations.

Negotiation Mode ● Automatic ○ Main ○ Aggressive

Encryption □ AES256 □ AES192 ☑ AES128 □ 3DES □ DES

Authentication ☑ SHA1 □ MD5

Integrity Hash ☑ AES ☑ SHA1 ☑ MD5

DH Group □ 5 ☑ 2 ☑ 1

SA Timeout 86400 <60-604800>Second

IPSec Parameters

Encapsulation Mode ● Automatic ○ Transport ○ Tunnel

Security Protocol ● ESP ○ AH ○ AH-ESP

ESP Encryption □ AES256 □ AES192 ☑ AES128 □ 3DES □ DES

ESP Authentication ☑ SHA1 □ MD5

PFS ● NONE ○ 5 ○ 2 ○ 1

SA Timeout

Based on Time 3600 <480-604800>Second

Based on Traffic 1843200 <0, 8000-4194303>KB

☑ **Dead Peer Detection (DPD)**

Detection Mode ● Periodic ○ On-Demand

Detection Interval 10 <10-3600>Second

Retry Interval 5 <2-60>Second

☑ **NAT Traversal**

d. Click **Apply**. The configuration of USG_A is complete.

- Configure USG_B.

1. Configure the basic parameters of the interfaces.

a. Choose **Network** > **Interface** > **Interface**.

b. In **Interface List**, click ✎ of GE0/0/1.

c. In **Interface List**, click ✎ of GE0/0/1.

d. On the **Modify GigabitEthernet Interface** page, configure the following parameters:

- Zone: trust
- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0

Other parameters are set to the default values.

e. Click **Apply**.

f. In **Interface List**, click ✎ of GE0/0/2.

g. On the **Modify GigabitEthernet Interface** page, configure the following parameters:

- Zone: untrust
- IP Address: 200.10.1.1
- Subnet Mask: 255.255.255.0

Other parameters are set to the default values.

h. Click **Apply**.

2. For the USG, configure interzone packet filtering to ensure normal network communication. For the USG BSR/HSR, this operation is not required.

a. Configure the security policy between the Local zone and the Untrust zone.

. Choose **Firewall** > **Security Policy** > **Local Policy**.

i. In **Local Policy**, click **Add** to configure the following parameters:

- Source Zone: untrust
- Source Address: 200.1.1.0/24
- Action: permit

ii. Click **Apply**.

b. Configure the security policy between the Trust zone and the Untrust zone.

. Choose **Firewall** > **Security Policy** > **Forward Policy**.

i. In **Forward Policy List**, click **Add** to configure the following parameters:

- Source Zone: trust
- Destination Zone: untrust
- Source Address: 192.168.1.0/24
- Destination Address: 10.1.1.0/24
- Action: permit

ii. Click **Apply**.

iii. Choose **Firewall** > **Security Policy** > **Forward Policy**.

iv. In **Forward Policy List**, click **Add** to configure the following parameters:

- Source Zone: untrust
- Destination Zone: trust
- Source Address: 10.1.1.0/24
- Destination Address: 192.168.1.0/24
- Action: permit

v. Click **Apply**.

3. configure a static route from USG_B to network A, with the next-hop IP address of 200.10.1.2.

a. Choose **Route** > **Static** > **Static Route**.

b. In **Static Route List**, click **Add**.

c. On the **Add Static Route** page, configure the following parameters:

- Destination Address: 10.1.1.0
- Mask: 255.255.255.0
- Next Hop: 200.10.1.2

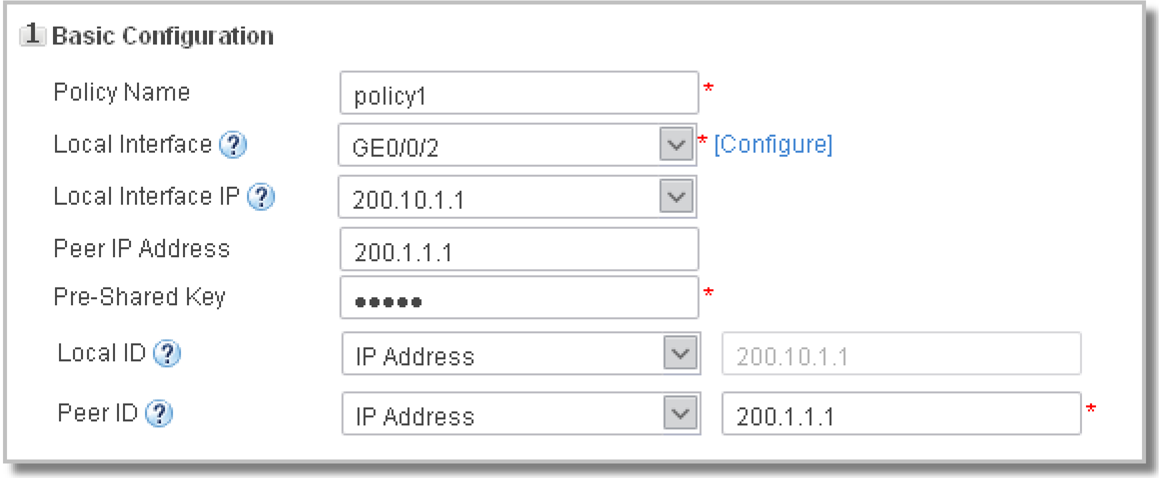
Other parameters are set to the default values.

d. Click **Apply**.

4. Configure the IPSec tunnel on USG_B.

a. Choose **VPN** > **IPSec** > **IPSec**, click **Add**, and set **Scenario** to **Site-to-site**.

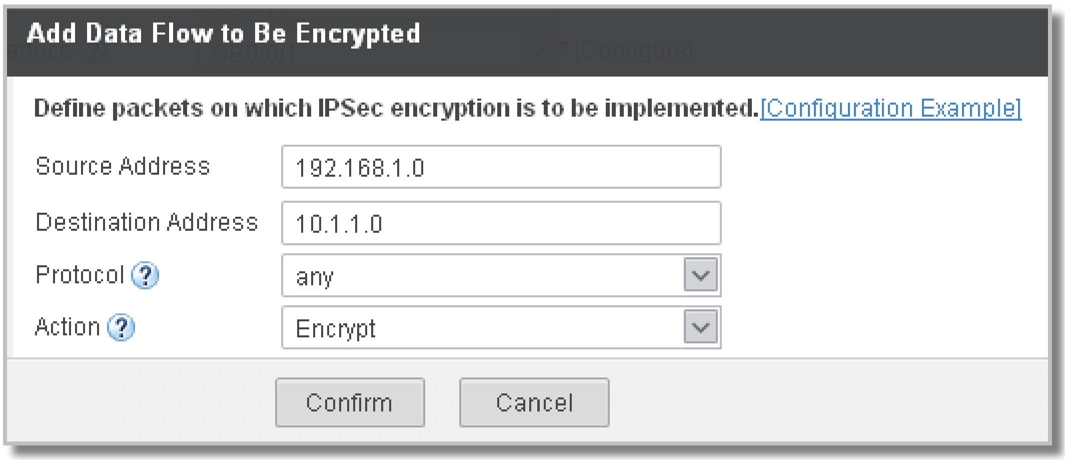
b. Configure the basic IPSec policy information, specify the remote gateway, and set the pre-shared key to abcd.



1 Basic Configuration

Policy Name	policy1	*
Local Interface ?	GE0/0/2	* [Configure]
Local Interface IP ?	200.10.1.1	
Peer IP Address	200.1.1.1	
Pre-Shared Key	●●●●●	*
Local ID ?	IP Address	200.10.1.1
Peer ID ?	IP Address	200.1.1.1 *

c. Under **Data Flow to Be Encrypted**, click **Add** to add a data flow as follows.



Add Data Flow to Be Encrypted

Define packets on which IPSec encryption is to be implemented.[Configuration Example]

Source Address: 192.168.1.0

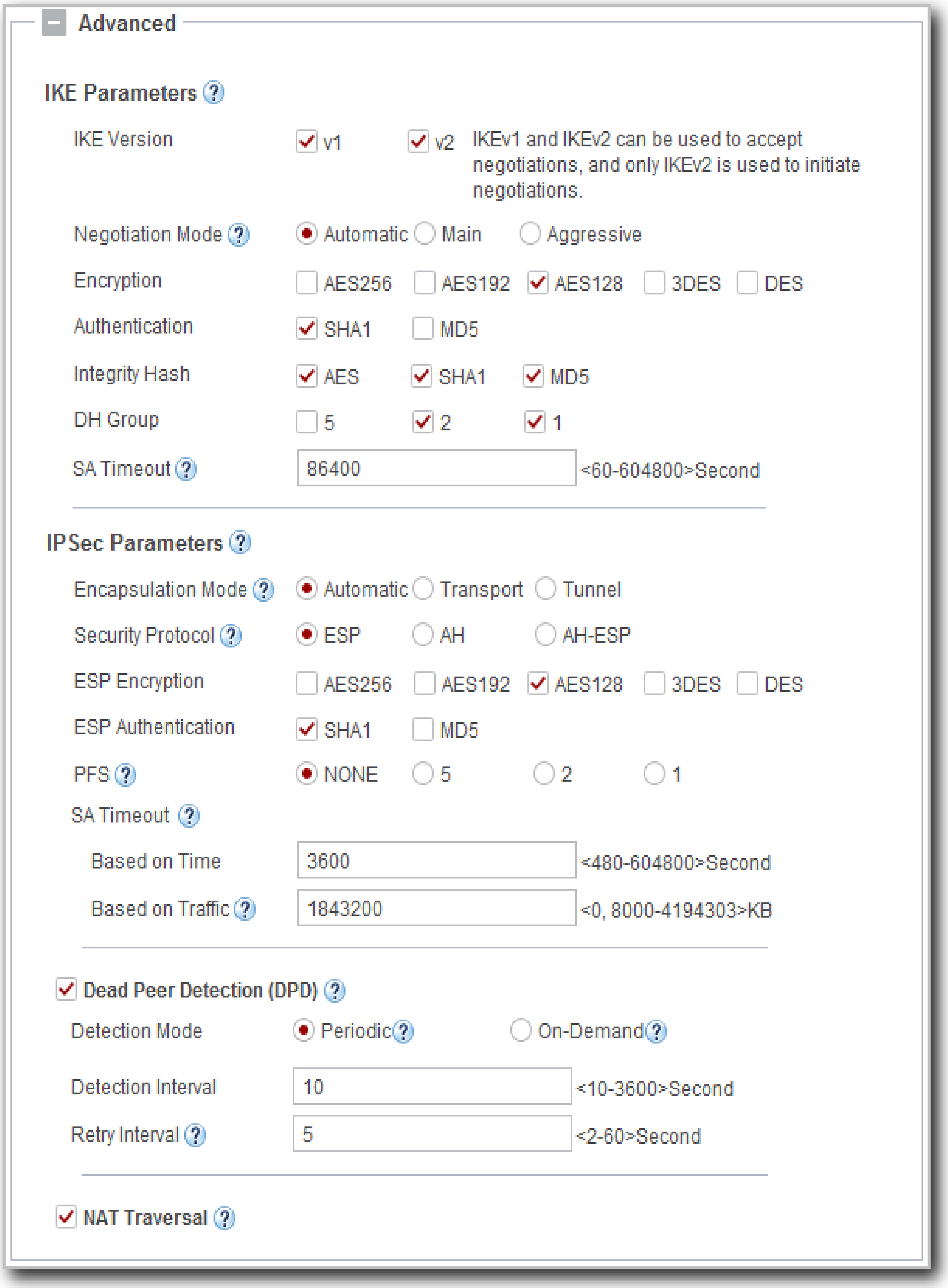
Destination Address: 10.1.1.0

Protocol: any

Action: Encrypt

d. Under **IKE/IPSec Proposal**, expand **Advanced**, and configure IPSec proposal as follows.

In this example, all proposal parameters are set to default values, as shown in the following figure. If you change the value of a parameter, you must ensure that the parameter settings are the same on both tunnel ends.



Advanced

IKE Parameters

IKE Version	☑ v1 ☑ v2	IKEv1 and IKEv2 can be used to accept negotiations, and only IKEv2 is used to initiate negotiations.
Negotiation Mode	● Automatic ○ Main ○ Aggressive	
Encryption	□ AES256 □ AES192 ☑ AES128 □ 3DES □ DES	
Authentication	☑ SHA1 □ MD5	
Integrity Hash	☑ AES ☑ SHA1 ☑ MD5	
DH Group	□ 5 ☑ 2 ☑ 1	
SA Timeout	86400	<60-604800>Second

IPSec Parameters

Encapsulation Mode	● Automatic ○ Transport ○ Tunnel	
Security Protocol	● ESP ○ AH ○ AH-ESP	
ESP Encryption	□ AES256 □ AES192 ☑ AES128 □ 3DES □ DES	
ESP Authentication	☑ SHA1 □ MD5	
PFS	● NONE ○ 5 ○ 2 ○ 1	
SA Timeout		
Based on Time	3600	<480-604800>Second
Based on Traffic	1843200	<0, 8000-4194303>KB

☑ Dead Peer Detection (DPD)

Detection Mode	● Periodic ○ On-Demand	
Detection Interval	10	<10-3600>Second
Retry Interval	5	<2-60>Second

☑ NAT Traversal

e. Click **Apply**. The configuration of USG_B is complete.

5.4 Testing

5.4.1 Verification

Access a host or server on network B from network A. The access succeeds.

On USG_A, choose **VPN** > **IPSec** > **Monitor** to display the established tunnels.

Policy Name	Status	Local Address	Peer Address
policy1	**IKE and IPSec negotiations succeed.**	200.1.1.1	200.10.1.1

On USG_B, choose **VPN** > **IPSec** > **Monitor** to display the established tunnels.

Policy Name	Status	Local Address	Peer Address
policy1	**IKE and IPSec negotiations succeed.**	200.10.1.1	200.1.1.1

5.5 Implementation of GRE Tunnel With Static Route

5.5.1 Configuration Roadmap

The configuration roadmaps for USG_A and USG_B are the same. The configuration roadmaps are as follows:

1. Configure the basic parameters of interfaces.
2. Create the GRE tunnel interfaces and configure the IP addresses, source address, and destination address of the GRE tunnel interfaces.
3. Enable the local policy and forwarding policy.
4. Configure the static routes and set the outbound interface as the tunnel interface so that the traffic is diverted to the tunnel.

5.5.2 Procedure

Configure USG_A.

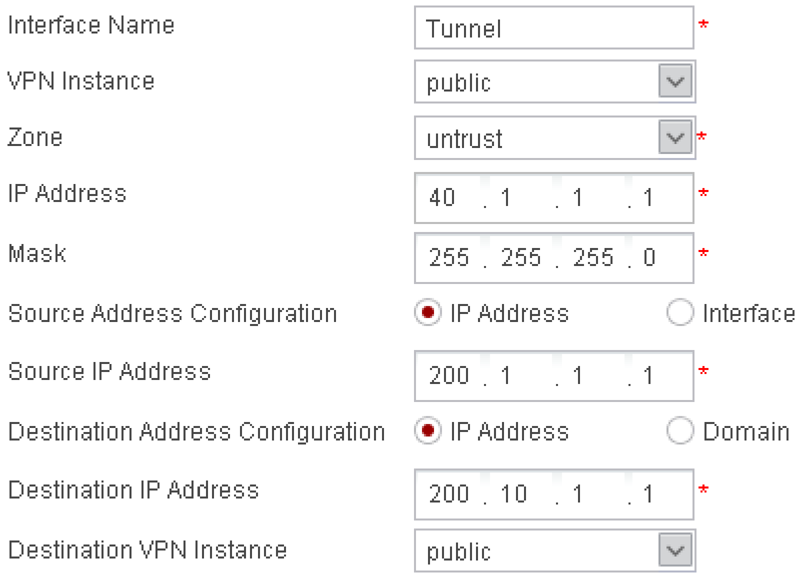
1. Configure the basic parameters of the interfaces.
    - a. Choose **Network** > **Interface** > **Interface**.
    - b. In **Interface List**, click 📝 of GE0/0/1.
    - c. On the **Modify GigabitEthernet Interface** page, configure the following parameters:
        - Zone: trust
        - IP Address: 10.1.1.1
        - Subnet Mask: 255.255.255.0

      Other parameters are set to the default values.
    - d. Click **Apply**.
    - e. In **Interface List**, click 📝 of GE0/0/2.
    - f. On the **Modify GigabitEthernet Interface** page, configure the following parameters:
        - Zone: untrust
        - IP Address: 200.1.1.1
        - Subnet Mask: 255.255.255.0

      Other parameters are set to the default values.
    - g. Click **Apply**.
2. Configure the GRE tunnel interfaces.
    - a. Choose **VPN** > **GRE** > **GRE**.

b. In **GRE Interface List**, click **Add**.

c. Configure GRE interface parameters, as shown Figure 16.



Interface Name	Tunnel *
VPN Instance	public
Zone	untrust *
IP Address	40 . 1 . 1 . 1 *
Mask	255 . 255 . 255 . 0 *
Source Address Configuration	● IP Address ○ Interface
Source IP Address	200 . 1 . 1 . 1 *
Destination Address Configuration	● IP Address ○ Domain
Destination IP Address	200 . 10 . 1 . 1 *
Destination VPN Instance	public

Figure 16: Configuring the GRE tunnel interface parameters on USG_A

1. For the USG, configure interzone packet filtering to ensure normal network communication. For the USG BSR/HSR, this operation is not required.

   a. Configure the security policy between the Local zone and the Untrust zone.

      i. Choose **Firewall** > **Security Policy** > **Local Policy**.

      ii. In **Local Policy**, click **Add** to configure the following parameters:

      - Source Zone: untrust
      - Source Address: 200.1.1.0/24
      - Action: permit

      iii. Click **Apply**.

   b. Configure the security policy between the Trust zone and the Untrust zone.

      i. Choose **Firewall** > **Security Policy** > **Forward Policy**.

      ii. In **Forward Policy List**, click **Add** to configure the following parameters:

      - Source Zone: trust

        - Destination Zone: untrust
        - Source Address: 10.1.1.0/24
        - Destination Address: 192.168.1.0/24
        - Action: permit

      iii. Click **Apply**.

      iv. In **Forward Policy List**, click **Add** to configure the following parameters:

        - Source Zone: untrust
        - Destination Zone: trust
        - Source Address: 192.168.1.0/24
        - Destination Address: 10.1.1.0/24
        - Action: permit

      v. Click **Apply**.

  2. Configure a static route from USG_A to network B, with the outbound interface being the GRE tunnel interface.

     a. Choose **Route** > **Static** > **Static Route**.

     b. In **Static Route List**, click **Add**.

     c. On **Add Static Route**, set the following parameters:

        - Destination Address: 192.168.1.0
        - Mask: 255.255.255.0
        - Interface: Tunnel

        Other parameters are set to the default values.

     d. Click **Apply**.

- Configure USG_B.

  1. Configure the basic parameters of the interfaces.

     a. Choose **Network** > **Interface** > **Interface**.

     b. In **Interface List**, click ✎ on GE0/0/1.

     c. On the **Modify GigabitEthernet Interface** page, configure the following parameters:

        - Zone: trust
        - IP Address: 192.168.1.1
        - Subnet Mask: 255.255.255.0

        Other parameters are set to the default values.

     d. Click **Apply**.

e. In **Interface List**, click ✎ that corresponds to GE0/0/2.

f. On **Modify GigabitEthernet Interface**, set the following parameters:

- Zone: untrust
- IP Address: 200.10.1.1
- Subnet Mask: 255.255.255.0

Other parameters are set to the default values.

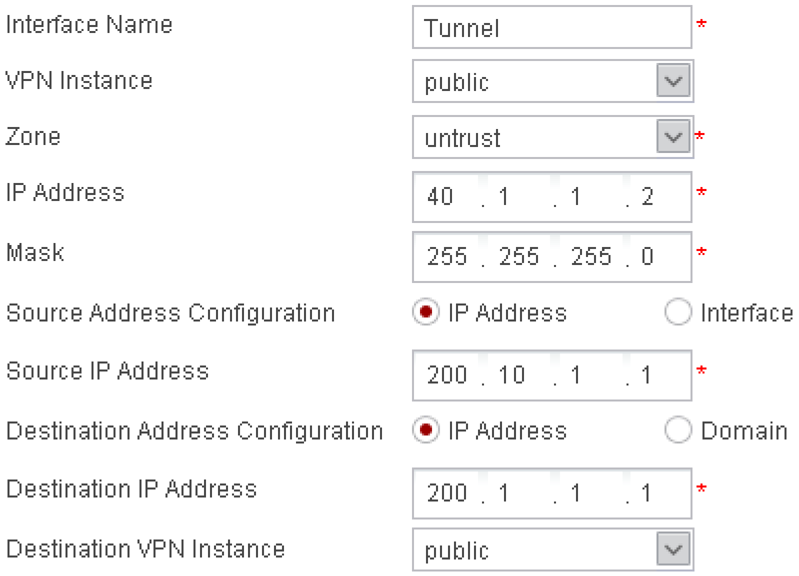
g. Click **Apply**.

2. Configure the GRE tunnel interfaces.

a. Choose **VPN** > **GRE** > **GRE**.

b. In **GRE Interface List**, click **Add**.

c. Configure the GRE tunnel interface parameters, as shown in Figure 17.



Interface Name	Tunnel *	
VPN Instance	public	
Zone	untrust *	
IP Address	40 . 1 . 1 . 2 *	
Mask	255 . 255 . 255 . 0 *	
Source Address Configuration	● IP Address	○ Interface
Source IP Address	200 . 10 . 1 . 1 *	
Destination Address Configuration	● IP Address	○ Domain
Destination IP Address	200 . 1 . 1 . 1 *	
Destination VPN Instance	public	

Figure 17: Configuring the GRE tunnel interface parameters on USG_B

1. For the USG, configure interzone packet filtering to ensure normal network communication. For the USG BSR/HSR, this operation is not required.

a. Configure the security policy between the Local zone and the Untrust zone.

i. Choose **Firewall** > **Security Policy** > **Local Policy**.

ii. In **Local Policy**, click **Add** to configure the following parameters:

- Source Zone: untrust
- Source Address: 200.1.1.0/24

- Action: permit

iii. Click **Apply**.

b. Configure the security policy between the Trust zone and the Untrust zone.

i. Choose **Firewall** > **Security Policy** > **Forward Policy**.

ii. In **Forward Policy List**, click **Add** to configure the following parameters:

- Source Zone: trust
- Destination Zone: untrust
- Source Address: 192.168.1.0/24
- Destination Address: 10.1.1.0/24
- Action: permit

iii. Click **Apply**.

iv. In **Forward Policy List**, click **Add** to configure the following parameters:

- Source Zone: untrust
- Destination Zone: trust
- Source Address: 10.1.1.0/24
- Destination Address: 192.168.1.0/24
- Action: permit

v. Click **Apply**.

2. Configure a static route from USG_B to network A, with the outbound interface being the GRE tunnel interface.

a. Choose **Route** > **Static** > **Static Route**.

b. In **Static Route List**, click **Add**.

c. On the **Add Static Route** page, configure the following parameters:

- Destination Address: 10.1.1.0
- Mask: 255.255.255.0
- Outbound Interface: Tunnel

Other parameters are set to the default values.

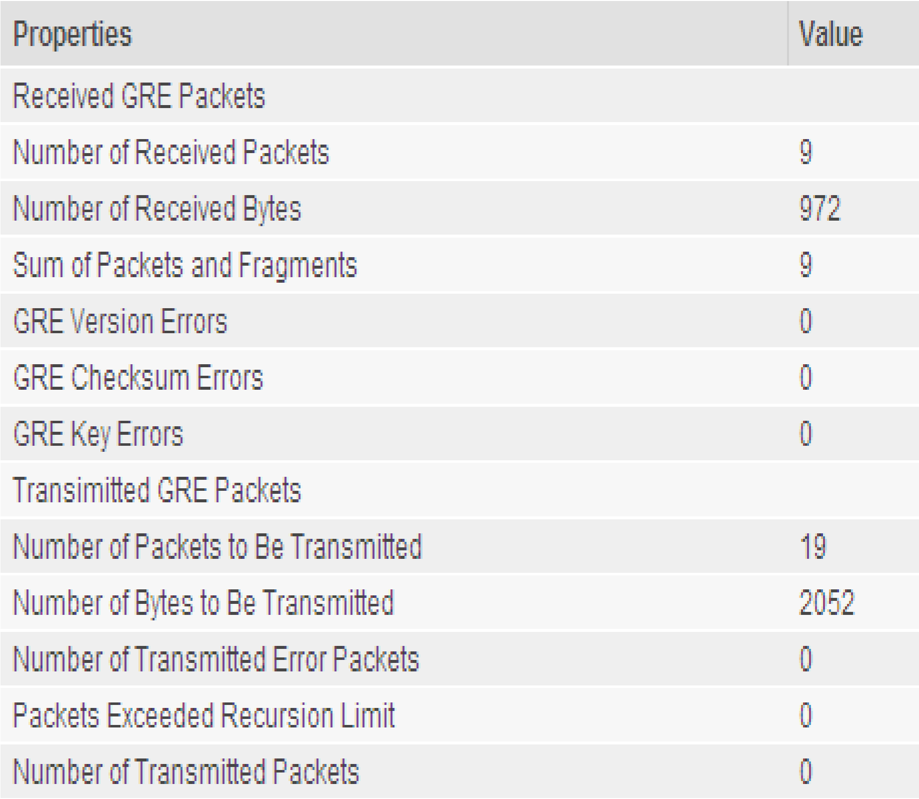
d. Click **Apply**.

5.6 Testing

5.6.1 Verification

1. Ping PC2 from PC1. The ping operation is successful.
2. Check whether the GRE tunnel is established on USG_A and USG_B. This section takes USG_A as an example.

   Choose **VPN** > **GRE** > **Monitor**. Check whether the number of encrypted or decrypted packets that are transmitted over the GRE tunnel exists. If the number of encrypted or decrypted packets exists, the GRE tunnel is successfully established, as shown in Figure 18 .



Properties	Value
Received GRE Packets	
Number of Received Packets	9
Number of Received Bytes	972
Sum of Packets and Fragments	9
GRE Version Errors	0
GRE Checksum Errors	0
GRE Key Errors	0
Transimitted GRE Packets	
Number of Packets to Be Transmitted	19
Number of Bytes to Be Transmitted	2052
Number of Transmitted Error Packets	0
Packets Exceeded Recursion Limit	0
Number of Transmitted Packets	0

Figure 18: Checking the GRE tunnel information on USG_A

5.7 Implementation of GER-over-IPSec Tunnel

5.7.1 Configuration Roadmap

For USG_A and USG_B, the configuration roadmap, which is the same, is as follows:

1. Complete the basic configurations for interfaces.
2. Create GRE tunnel interfaces and configure an IP address, source IP address, and destination IP address for the interfaces.
3. Enable the local policy and the forwarding policy.
4. Configure a static route and specify the outbound interface as the GRE tunnel interface to divert traffic to the tunnel.
5. Configure the IPSec policy, including basic IPSec policy information, data flow to be protected by IPSec, and proposal parameters for security association negotiation.

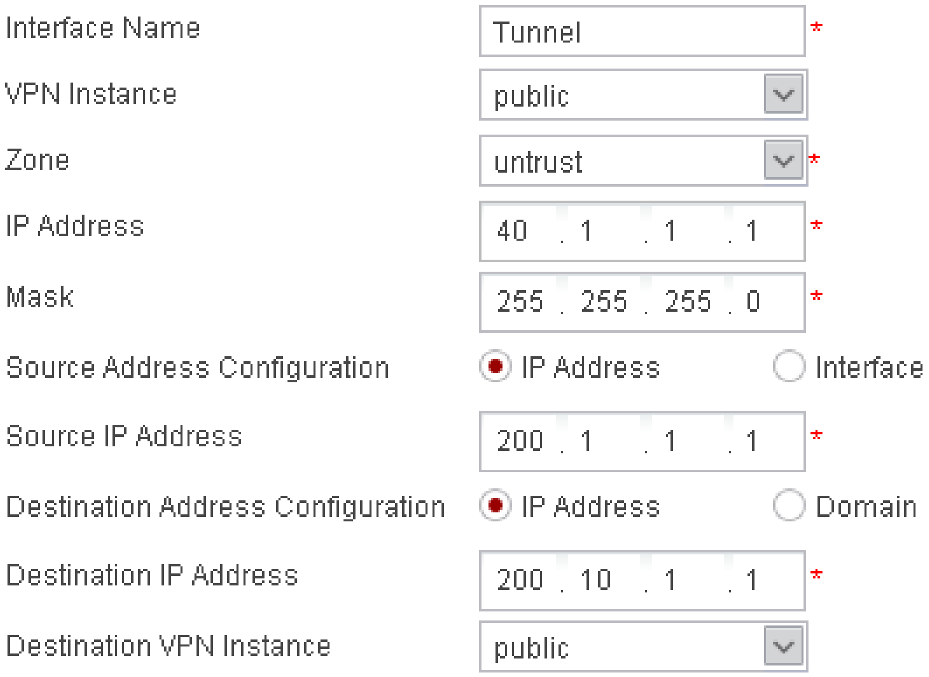
5.7.2 Procedure

Configure USG_A.

1. Configure the basic parameters of the interfaces.
   a. Choose **Network** > **Interface** > **Interface**.
   b. In **Interface List**, click 📝 of GE0/0/1.
   c. On the **Modify GigabitEthernet Interface** page, configure the following parameters:
      - Zone: trust
      - IP Address: 10.1.1.1
      - Subnet Mask: 255.255.255.0

      Other parameters are set to the default values.
   d. Click **Apply**.
   e. In **Interface List**, click 📝 of GE0/0/2.
   f. On the **Modify GigabitEthernet Interface** page, configure the following parameters:
      - Zone: untrust
      - IP Address: 200.1.1.1
      - Subnet Mask: 255.255.255.0

      Other parameters are set to the default values.
   g. Click **Apply**.
2. Configure GRE tunnel interfaces.
   a. Choose **VPN** > **GRE** > **GRE**.
   b. In **GRE Interface List**, click **Add**.
   c. Configure GRE tunnel interface parameters, as shown Figure 19.



Interface Name	Tunnel	*
VPN Instance	public	
Zone	untrust	*
IP Address	40 . 1 . 1 . 1	*
Mask	255 . 255 . 255 . 0	*
Source Address Configuration	● IP Address	○ Interface
Source IP Address	200 . 1 . 1 . 1	*
Destination Address Configuration	● IP Address	○ Domain
Destination IP Address	200 . 10 . 1 . 1	*
Destination VPN Instance	public	

Figure 19: Configuring a GRE tunnel interface on USG_A

1. For the USG, configure interzone packet filtering to ensure normal network communication. For the USG BSR/HSR, this operation is not required.

   a. Configure the security policy between the Local zone and the Untrust zone.

      i. Choose **Firewall** > **Security Policy** > **Local Policy**.

      ii. In **Local Policy**, click **Add** to configure the following parameters:

      - Source Zone: untrust
      - Source Address: 200.10.1.0/24
      - Action: permit

      iii. Click **Apply**.

   b. Configure the security policy between the Trust zone and the Untrust zone.

      i. Choose **Firewall** > **Security Policy** > **Forward Policy**.

      ii. In **Forward Policy List**, click **Add** to configure the following parameters:

      - Source Zone: trust
      - Destination Zone: untrust
      - Source Address: 10.1.1.0/24
      - Destination Address: 192.168.1.0/24
      - Action: permit

      iii. Click **Apply**.

iv. Choose **Firewall** > **Security Policy** > **Forward Policy**.

v. In **Forward Policy List**, click **Add** to configure the following parameters:

- Source Zone: untrust
- Destination Zone: trust
- Source Address: 192.168.1.0/24
- Destination Address: 10.1.1.0/24
- Action: permit

vi. Click **Apply**.

2. Configure a static route from USG_A to network B, with the outbound interface being the GRE tunnel interface.

   a. Choose **Route** > **Static** > **Static Route**.

   b. In **Static Route List**, click **Add**.

   c. On the **Add Static Route** page, configure the following parameters:

      - Destination Address: 192.168.1.0
      - Mask: 255.255.255.0
      - Interface: Tunnel

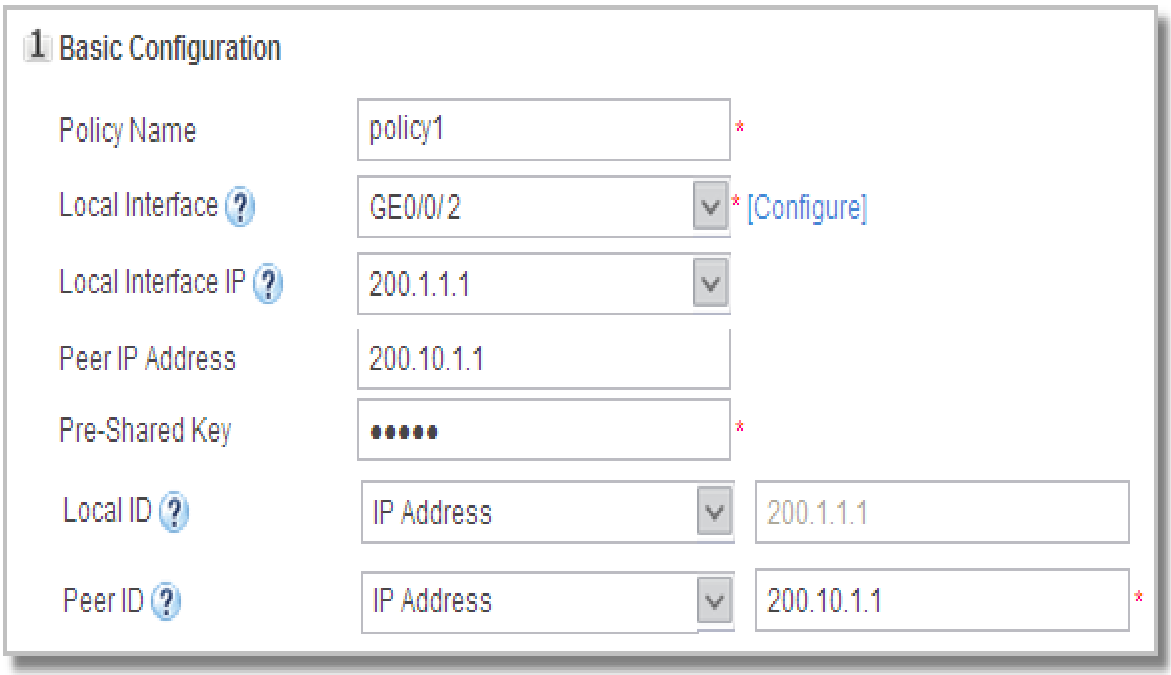
      Other parameters are set to the default values.

   d. Click **Apply**.

3. Configure the IPSec tunnel on USG_A.

   a. Choose **VPN** > **IPSec** > **IPSec**, click **Add**, and set **Scenario** to **Site-to-site**.

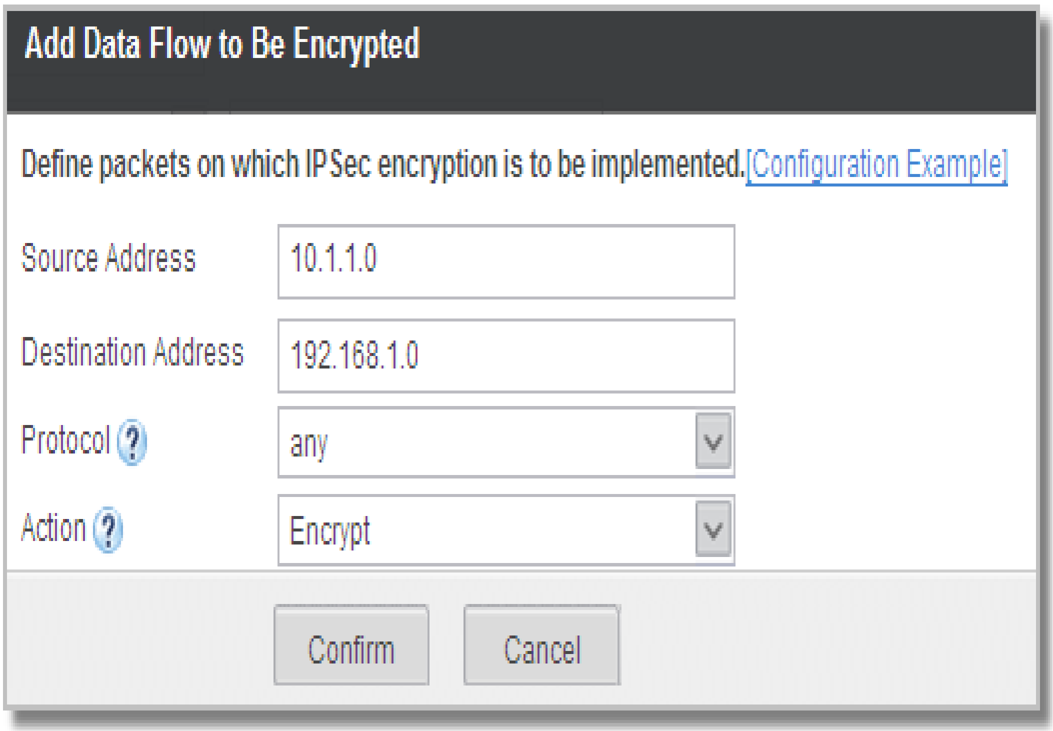
   b. Configure the basic IPSec policy information, specify the remote gateway, and set the pre-shared key to abcde.



1 Basic Configuration

Policy Name	policy1	*
Local Interface	GE0/0/2	* [Configure]
Local Interface IP	200.1.1.1	
Peer IP Address	200.10.1.1	
Pre-Shared Key	●●●●●	*
Local ID	IP Address	200.1.1.1
Peer ID	IP Address	200.10.1.1 *

c. Under **Data Flow to Be Encrypted**, click **Add** to add a data flow as follows.



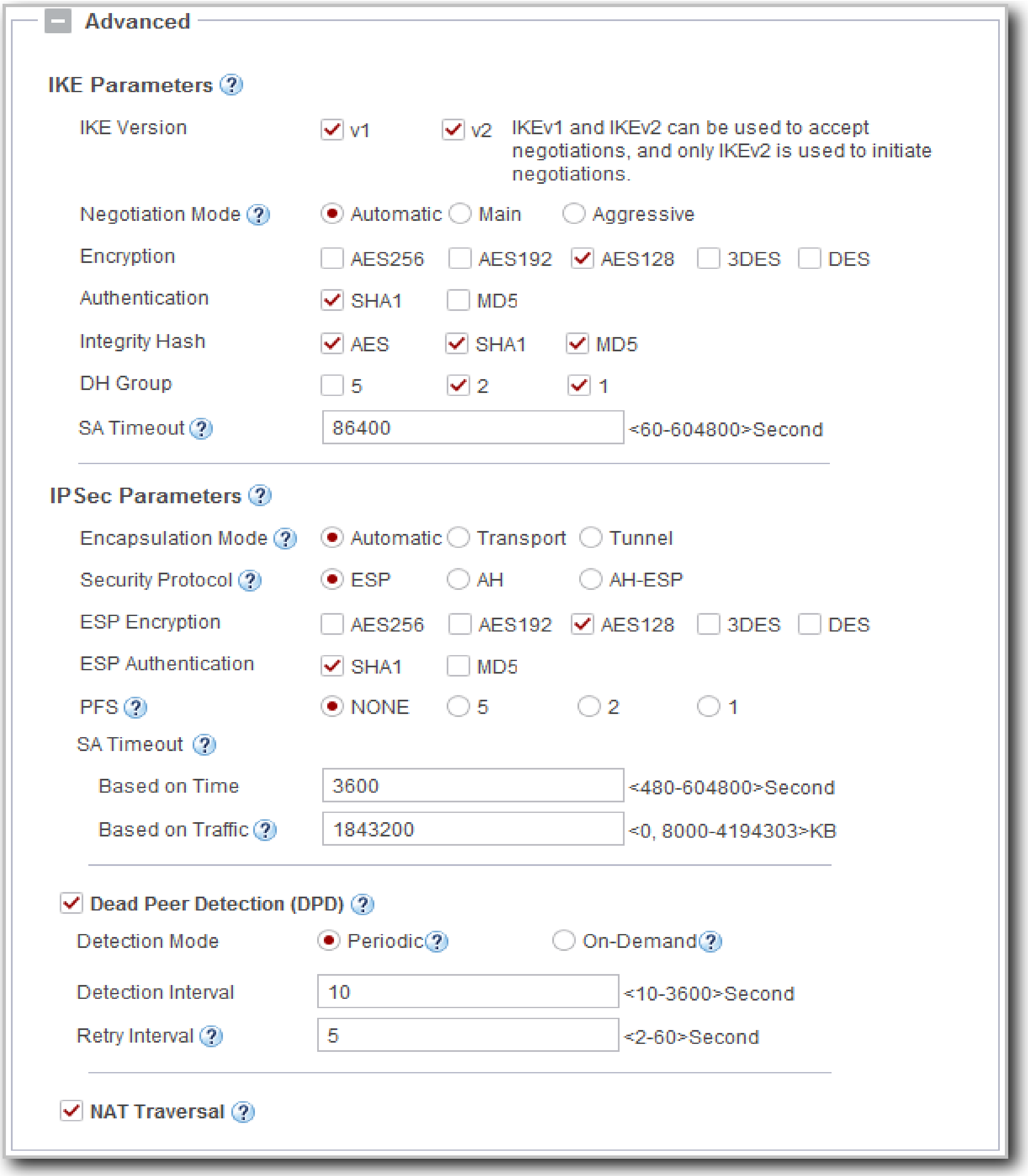
Add Data Flow to Be Encrypted

Define packets on which IPSec encryption is to be implemented.[Configuration Example]

Source Address	10.1.1.0
Destination Address	192.168.1.0
Protocol	any
Action	Encrypt

a. Under **IKE/IPSec Proposal**, expand **Advanced**, and configure IPSec proposal as follows.

In this example, all proposal parameters are set to default values, as shown in the following figure. If you change the value of a parameter, you must ensure that the parameter settings are the same on both tunnel ends.



Advanced

IKE Parameters ?

IKE Version ☑ v1 ☑ v2 IKEv1 and IKEv2 can be used to accept negotiations, and only IKEv2 is used to initiate negotiations.

Negotiation Mode ? ● Automatic ○ Main ○ Aggressive

Encryption □ AES256 □ AES192 ☑ AES128 □ 3DES □ DES

Authentication ☑ SHA1 □ MD5

Integrity Hash ☑ AES ☑ SHA1 ☑ MD5

DH Group □ 5 ☑ 2 ☑ 1

SA Timeout ? 86400 <60-604800>Second

IPSec Parameters ?

Encapsulation Mode ? ● Automatic ○ Transport ○ Tunnel

Security Protocol ? ● ESP ○ AH ○ AH-ESP

ESP Encryption □ AES256 □ AES192 ☑ AES128 □ 3DES □ DES

ESP Authentication ☑ SHA1 □ MD5

PFS ? ● NONE ○ 5 ○ 2 ○ 1

SA Timeout ?

Based on Time 3600 <480-604800>Second

Based on Traffic ? 1843200 <0, 8000-4194303>KB

☑ Dead Peer Detection (DPD) ?

Detection Mode ● Periodic? ○ On-Demand?

Detection Interval 10 <10-3600>Second

Retry Interval ? 5 <2-60>Second

☑ NAT Traversal ?

a. Click **Apply**. The configuration of USG_A is complete.

Configure USG_B.

1. Configure the basic parameters of the interfaces.

a. Choose **Network** > **Interface** > **Interface**.

b. In **Interface List**, click 📝 on GE0/0/1.

c. On the **Modify GigabitEthernet Interface** page, configure the following parameters:

- Zone: trust
- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0

Other parameters are set to the default values.

d. Click **Apply**.

e. In **Interface List**, click 📝 on GE0/0/2.

f. On the **Modify GigabitEthernet Interface** page, configure the following parameters:

- Zone: untrust
- IP Address: 200.10.1.1
- Subnet Mask: 255.255.255.0

Other parameters are set to the default values.

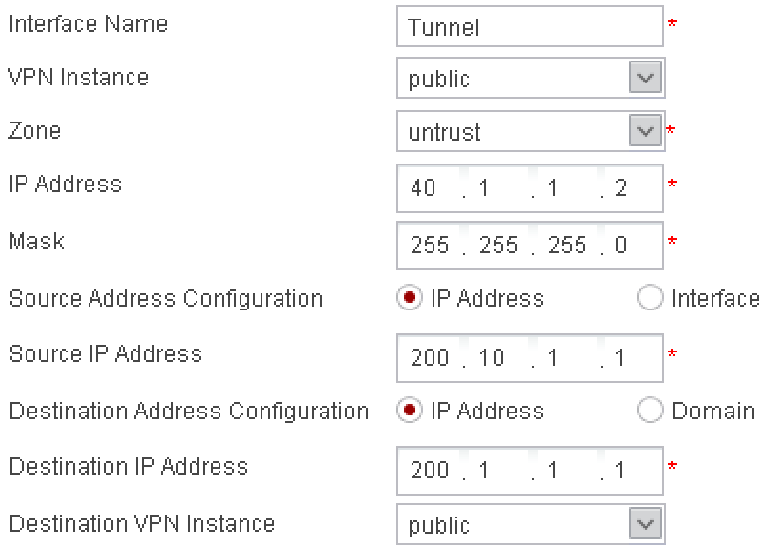
g. Click **Apply**.

2. Configure GRE tunnel interfaces.

a. Choose **VPN** > **GRE** > **GRE**.

b. In **GRE Interface List**, click **Add**.

c. Configure GRE interface parameters, as shown Figure 20.



Interface Name	Tunnel *
VPN Instance	public
Zone	untrust *
IP Address	40 . 1 . 1 . 2 *
Mask	255 . 255 . 255 . 0 *
Source Address Configuration	● IP Address ○ Interface
Source IP Address	200 . 10 . 1 . 1 *
Destination Address Configuration	● IP Address ○ Domain
Destination IP Address	200 . 1 . 1 . 1 *
Destination VPN Instance	public

Figure 20: Configuring a GRE tunnel interface on USG_B

1. For the USG, configure interzone packet filtering to ensure normal network communication. For the USG BSR/HSR, this operation is not required.
    a. Configure the security policy between the Local zone and the Untrust zone.
        i. Choose **Firewall** > **Security Policy** > **Local Policy**.
        ii. In **Local Policy**, click **Add** to configure the following parameters:
            - Source Zone: untrust
            - Source Address: 200.1.1.0/24
            - Action: permit
        iii. Click **Apply**.
    b. Configure the security policy between the Trust zone and the Untrust zone.
        i. Choose **Firewall** > **Security Policy** > **Forward Policy**.
        ii. In **Forward Policy List**, click **Add** to configure the following parameters:
            - Source Zone: trust
            - Destination Zone: untrust
            - Source Address: 192.168.1.0/24
            - Destination Address: 10.1.1.0/24
            - Action: permit
        iii. Click **Apply**.
        iv. Choose **Firewall** > **Security Policy** > **Forward Policy**.
        v. In **Forward Policy List**, click **Add** to configure the following parameters:
            - Source Zone: untrust
            - Destination Zone: trust
            - Source Address: 10.1.1.0/24
            - Destination Address: 192.168.1.0/24
            - Action: permit
        vi. Click **Apply**.
2. Configure a static route from USG_B to network A, with the outbound interface being the GRE tunnel interface.
    a. Choose **Route** > **Static** > **Static Route**.
    b. In **Static Route List**, click **Add**.
    c. On the **Add Static Route** page, configure the following parameters:
        - Destination Address: 10.1.1.0
        - Mask: 255.255.255.0
        - Interface: Tunnel

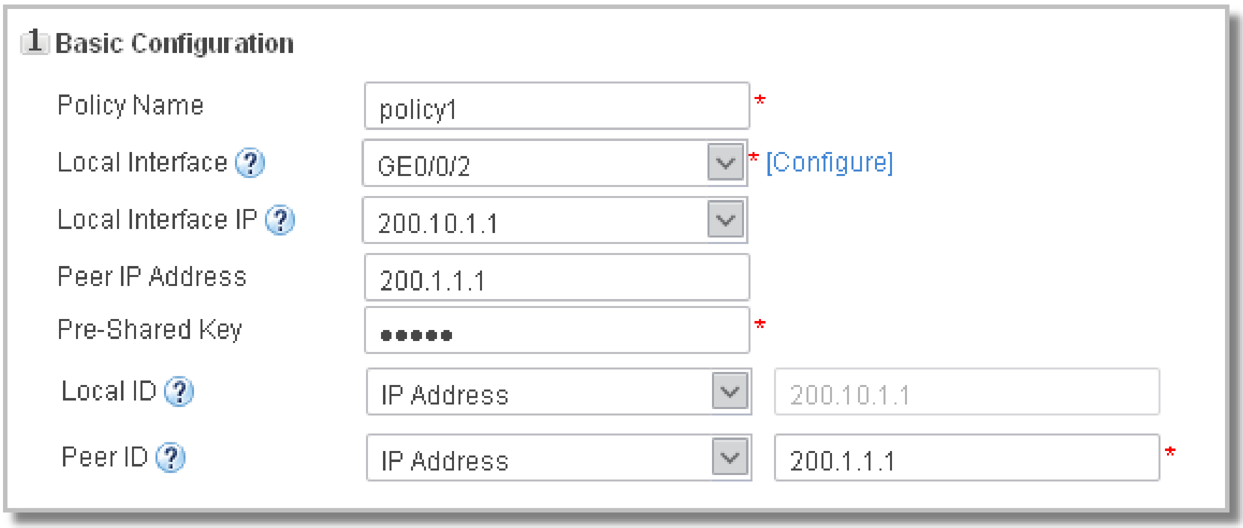
Other parameters are set to the default values.

d. Click **Apply**.

3. Configure the IPSec tunnel on USG_B.

a. Choose **VPN** > **IPSec** > **IPSec**, click **Add**, and set **Scenario** to **Site-to-site**.

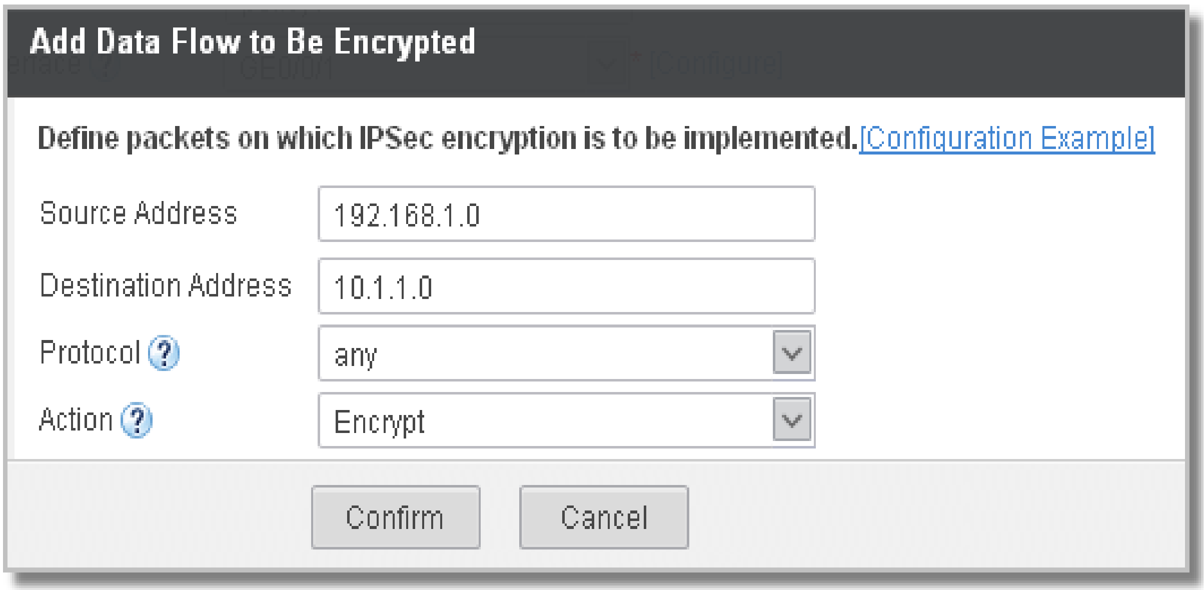
b. Configure the basic IPSec policy information, specify the remote gateway, and set the pre-shared key to abcde.



1 Basic Configuration

Policy Name	policy1	*
Local Interface ?	GE0/0/2	* [Configure]
Local Interface IP ?	200.10.1.1	
Peer IP Address	200.1.1.1	
Pre-Shared Key	●●●●●	*
Local ID ?	IP Address	200.10.1.1
Peer ID ?	IP Address	200.1.1.1 *

c. Under **Data Flow to Be Encrypted**, click **Add** to add a data flow as follows.



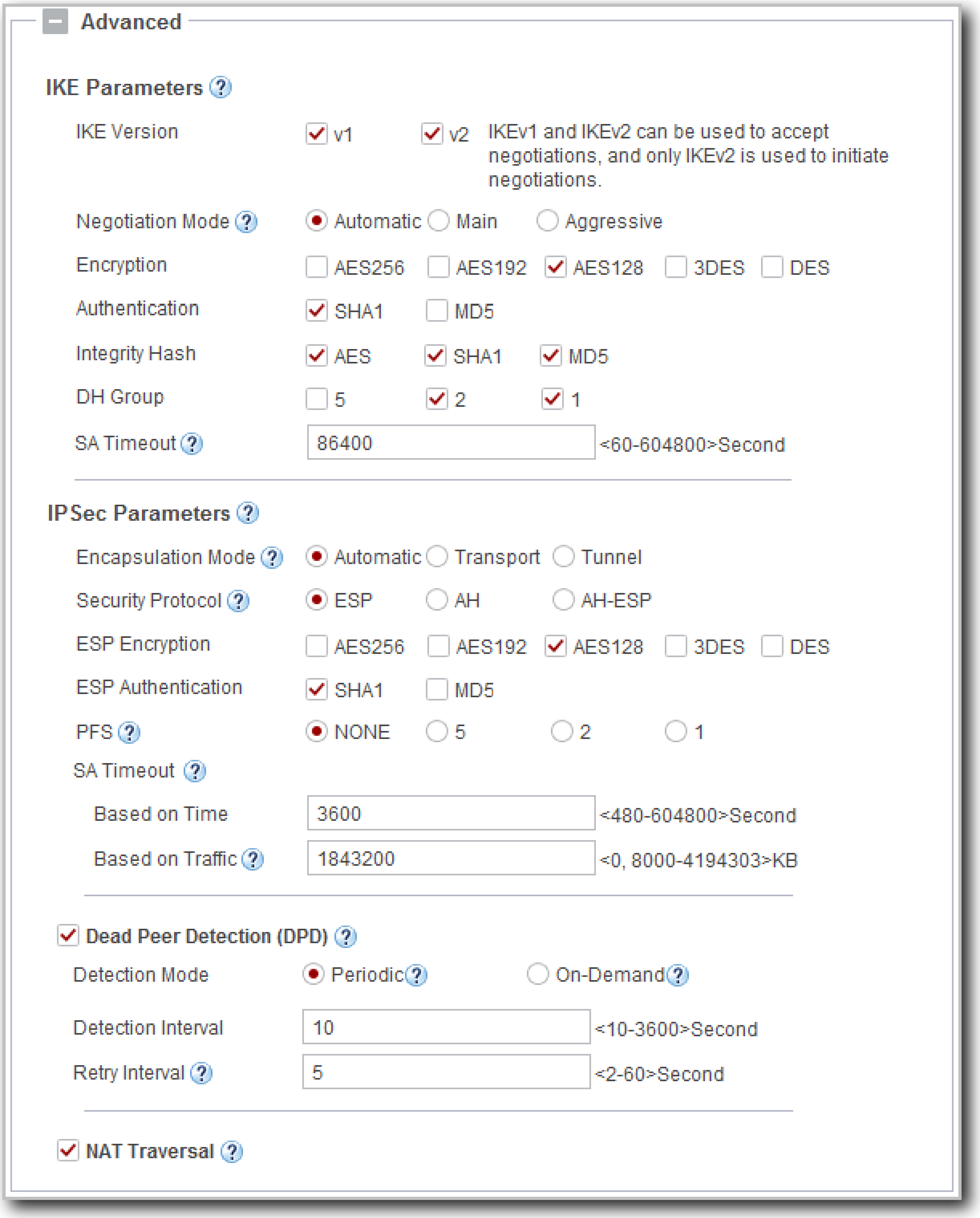
Add Data Flow to Be Encrypted

Define packets on which IPSec encryption is to be implemented.[Configuration Example]

Source Address	192.168.1.0
Destination Address	10.1.1.0
Protocol ?	any
Action ?	Encrypt

d. Under **IKE/IPSec Proposal**, expand **Advanced**, and configure IPSec proposal as follows.

In this example, all proposal parameters are set to default values, as shown in the following figure. If you change the value of a parameter, you must ensure that the parameter settings are the same on both tunnel ends.



Advanced

IKE Parameters

IKE Version ☑ v1 ☑ v2 IKEv1 and IKEv2 can be used to accept negotiations, and only IKEv2 is used to initiate negotiations.

Negotiation Mode ● Automatic ○ Main ○ Aggressive

Encryption □ AES256 □ AES192 ☑ AES128 □ 3DES □ DES

Authentication ☑ SHA1 □ MD5

Integrity Hash ☑ AES ☑ SHA1 ☑ MD5

DH Group □ 5 ☑ 2 ☑ 1

SA Timeout 86400 <60-604800>Second

IPSec Parameters

Encapsulation Mode ● Automatic ○ Transport ○ Tunnel

Security Protocol ● ESP ○ AH ○ AH-ESP

ESP Encryption □ AES256 □ AES192 ☑ AES128 □ 3DES □ DES

ESP Authentication ☑ SHA1 □ MD5

PFS ● NONE ○ 5 ○ 2 ○ 1

SA Timeout

Based on Time 3600 <480-604800>Second

Based on Traffic 1843200 <0, 8000-4194303>KB

☑ **Dead Peer Detection (DPD)**

Detection Mode ● Periodic ○ On-Demand

Detection Interval 10 <10-3600>Second

Retry Interval 5 <2-60>Second

☑ **NAT Traversal**

e. Click **Apply**. The configuration of USG_B is complete.

5.8 Testing

5.8.1 Verification

Access a host or server on network B from network A. The access succeeds.

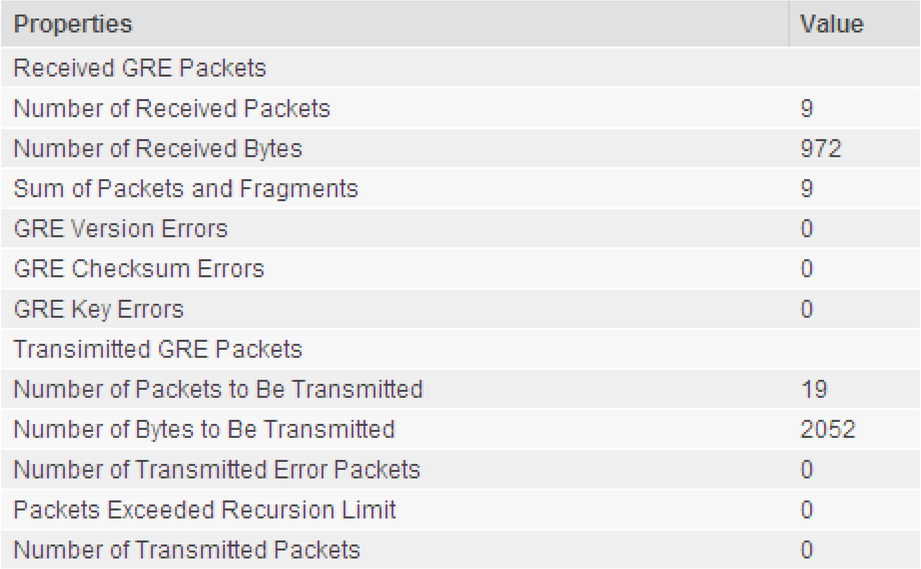
On USG_A, choose **VPN** > **IPSec** > **Monitor** to display the established tunnels.

Policy Name	Status	Local Address	Peer Address
policy1	**IKE and IPSec negotiations succeed.**	200.1.1.1	200.10.1.1

On USG_B, choose **VPN** > **IPSec** > **Monitor** to display the established tunnels.

Policy Name	Status	Local Address	Peer Address
policy1	**IKE and IPSec negotiations succeed.**	200.10.1.1	200.1.1.1

Choose **VPN** > **GRE** > **Monitor** to check the GRE tunnel establishment on USG_A and USG_B. For example, on USG_A, you can view GRE capsulated and decapsulated packets, which indicates that the GRE tunnel is established successfully. See Figure 21 .



Properties	Value
Received GRE Packets	
Number of Received Packets	9
Number of Received Bytes	972
Sum of Packets and Fragments	9
GRE Version Errors	0
GRE Checksum Errors	0
GRE Key Errors	0
Transimitted GRE Packets	
Number of Packets to Be Transmitted	19
Number of Bytes to Be Transmitted	2052
Number of Transmitted Error Packets	0
Packets Exceeded Recursion Limit	0
Number of Transmitted Packets	0

Figure 21: Viewing information about the GRE tunnel on USG_A

CHAPTER 6

CASE STUDY

6.1 Manage Air

6.1.1 Problem of Statement

Traffic Diversion is not working properly in case of network down.

6.1.2 Requirement

- Traffics from the respective interfaces are forwarded to the specific internet link (Worldlink or Mercantile).
- Both internet link (Worldlink and Mercantile) should be used and if one link fails all the traffic are forwarded through another link.

6.1.3 Product Overview

We use the Secospace USG2110-F series of Huawei production to meet the above requirements. This series integrates security functions including IPS, AV, URL filtering, application control and content filtering and other functions such as routing, switching, VPN, bandwidth management and other networking protection providing a reliable and secure network for different enterprises.

6.1.4 Design

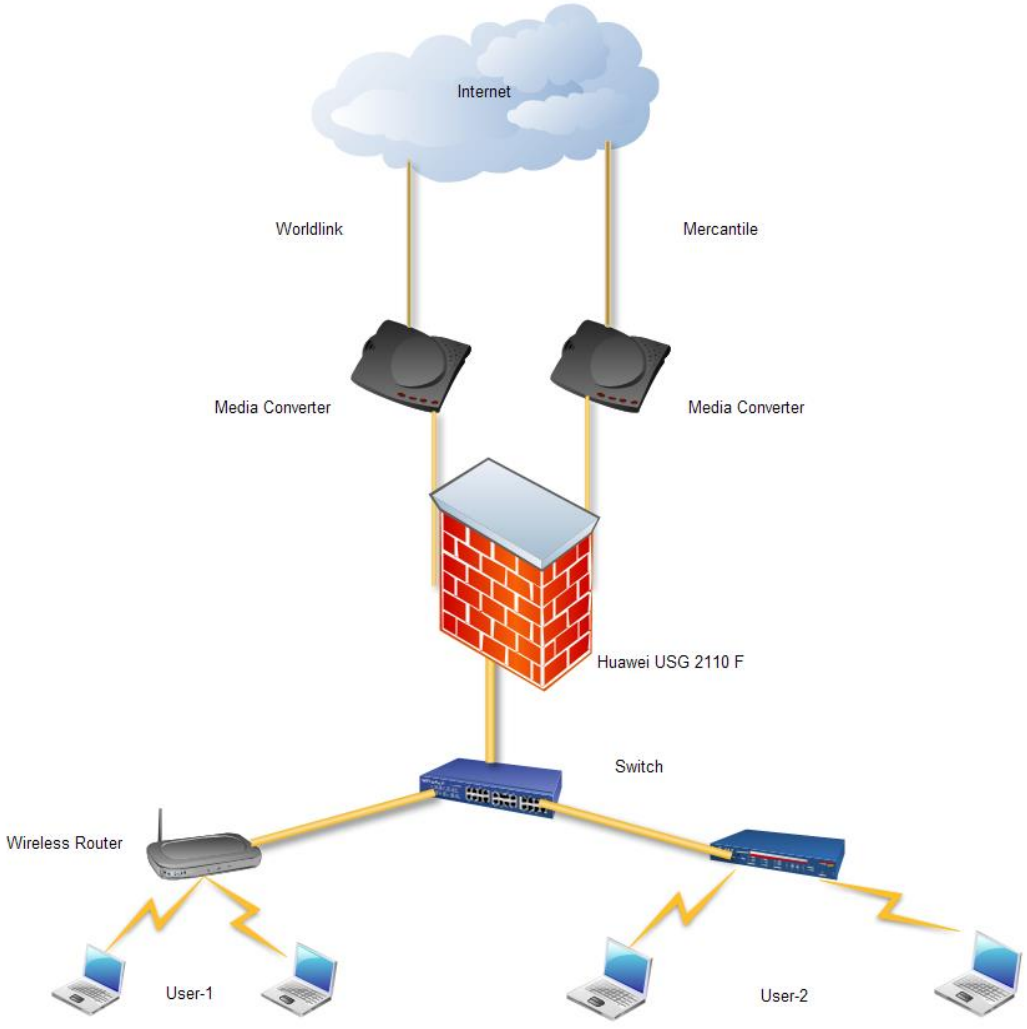


Figure 22: Network Design of Manage Air

6.1.5 Implementation and Testing

- Locate power supply: locate Installation position, Check ISP Link
- Configure the basic setup for internet access: DNS, DHCP, Routing, IP Address Routing
- Assign Firewall Zone to Network: LAN-Trust, Wan-Untrust
- Configure Policy Based Route(PBR): User1-Worldlink and User2-Mercantile
- Configure IP Links to check whether the internet links are up or not

CHAPTER 7

CONCLUSION

The internship duration in DOPL was very worthy to us as we got a secure and sound environment to learn about different fields in networking. We got a chance to test our theoretical knowledge and get in-depth practical knowledge. During our internship period we got many concepts about following fields:

- Different technologies and equipment used in networking.
- Security mechanisms in network
- Interaction with different personnel.

Our internship was very beneficial and meaningful as we learnt about the different changing trends in Information Technology world. Also we got knowledge about dealing with challenging circumstances including organization discipline and time. Overall this internship program has helped us gain professional experience enhancing my interpersonal, group working and communicational skills.

BIBLIOGRAPHY

- HedEx Lite of Huawei Technologies Co. Ltd.
- Internet:http://www.dopl.com.np/
- Internet:http://www.huawei.com/en/
- en.wikipedia .org/wiki/internship