NSFOCUS WAF V6.0
Deployment Guide

Version: V6.0R07F00 (2018-04-25)

© 2020 NSFOCUS

■ Copyright © 2018 NSFOCUS Technologies, Inc. All rights reserved.

Unless otherwise stated, **NSFOCUS Technologies, Inc.** holds the copyright for the content of this document, including but not limited to the layout, figures, photos, methods, and procedures, which are protected under the intellectual property and copyright laws. No part of this publication may be reproduced or quoted, in any form or by any means, without prior written permission of **NSFOCUS Technologies, Inc.**

Contents

Preface **1**
Scope 1
Audience 1
Organization 1
Conventions 2
Customer Support 2
1 Deployment Modes **3**
1.1 In-Path Deployment 3
1.1.1 In-Path Deployment with Out-of-Band Management 3
1.1.2 In-Path Deployment with In-Band Management 4
1.2 Out-of-Path Deployment 5
1.3 Reverse Proxy Mode 6
1.4 Mirroring Deployment 7
1.5 Comparison Among Deployment Modes 8
2 Deployment Principles **10**
2.1 Out-of-Path Deployment 10
2.1.1 Traffic Diversion 10
2.1.2 Layer 2 Injection 10
2.1.3 Crossover Injection 14
2.1.4 PBR Injection 16
2.2 One-Arm Reverse Proxy Deployment 20
3 Configuration Examples **23**
3.1 Out-of-Path Deployment 23
3.1.1 Diversion via Static Route 23
3.1.2 Layer 2 Injection 25
3.1.3 Crossover Injection 35
3.1.4 PBR Injection 37
3.2 One-Arm Traditional Reverse Proxy 61
3.3 Mirroring Deployment 64
4 HA Configuration **69**
4.1 Active-Active Mode via Port Channel 69
4.2 Active-Active Mode via OSPF 72

4.3 Master/Slave Mode....76

5 VRRP Configuration....82

5.1 Configuring a Single VRRP Group....82

5.2 Configuring Multiple VRRP Groups....89

A Default Parameters....95

A.1 Default Settings of the Management Interface....95

A.2 Default Accounts....95

A.3 Communication Parameters of Console Port....95

Figures

Figure 1-1 In-Path deployment — out-of-band management topology 4
Figure 1-2 In-Path Deployment — in-band management topology 5
Figure 1-3 Out-of-path deployment topology 6
Figure 1-4 Reverse proxy deployment topology 7
Figure 1-5 Mirroring deployment topology 8
Figure 2-1 Layer 2 injection — downlink traffic 11
Figure 2-2 Layer 2 injection — uplink traffic 13
Figure 2-3 Crossover injection — downlink traffic 15
Figure 2-4 Crossover injection — uplink traffic 16
Figure 2-5 PBR injection — downlink traffic 17
Figure 2-6 PBR injection — uplink traffic 19
Figure 2-7 One-arm reverse proxy mode — downlink traffic 20
Figure 2-8 One-arm reverse proxy mode — uplink traffic 22
Figure 3-1 Diversion via static route — Work Group Management page 24
Figure 3-2 Diversion via static route — editing interface G1/4 configuration 25
Figure 3-3 Layer 2 injection — topology 26
Figure 3-4 Layer 2 injection — Work Group Management page 28
Figure 3-5 Layer 2 injection — creating a work group 29
Figure 3-6 Layer 2 injection — new work group on the Work Group Management page 30
Figure 3-7 Layer 2 injection — editing diversion interface configuration 31
Figure 3-8 Layer 2 injection — editing injection interface configuration 32
Figure 3-9 Layer 2 injection — adding subinterface 1 32
Figure 3-10 Layer 2 injection — adding subinterface 2 33
Figure 3-11 Layer 2 injection — two subinterfaces of the injection interface 34
Figure 3-12 Layer 2 injection — View Forwarding Routing Table dialog box 35
Figure 3-13 Crossover injection — topology 36
Figure 3-14 Layer 3 interface injection — topology 38

Figure 3-15 Layer 3 interface injection — Work Group Management page 41
Figure 3-16 Layer 3 interface injection — Create Work Group dialog box 41
Figure 3-17 Layer 3 interface injection — new work group on the Work Group Management page 42
Figure 3-18 Layer 3 interface injection — editing diversion interface configuration.....43
Figure 3-19 Layer 3 interface injection — editing injection interface configuration 43
Figure 3-20 Layer 3 interface injection — interface configuration on the Work Group Management page 44
Figure 3-21 Layer 3 interface injection — editing a work group 45
Figure 3-22 Layer 3 Interface injection — adding an injection route.....46
Figure 3-23 Layer 3 trunk injection — topology.....47
Figure 3-24 Layer 3 trunk injection — Work Group Management page 50
Figure 3-25 Layer 3 trunk injection — Create Work Group dialog box 50
Figure 3-26 Layer 3 trunk injection — new work group on the Work Group Management page 51
Figure 3-27 Layer 3 trunk injection — editing the diversion interface.....52
Figure 3-28 Layer 3 trunk injection — editing the injection interface 52
Figure 3-29 Layer 3 trunk injection — adding a subinterface.....53
Figure 3-30 One-Arm layer 3 injection — topology 54
Figure 3-31 One-arm layer 3 injection — Work Group Management page 56
Figure 3-32 One-arm layer 3 injection — Create Work Group dialog box 57
Figure 3-33 One-arm layer 3 injection — new work group on the Work Group Management page 57
Figure 3-34 One-arm layer 3 injection — editing interface configuration.....58
Figure 3-35 One-arm layer 3 injection — interface configuration 59
Figure 3-36 One-arm layer 3 injection — editing a work group 60
Figure 3-37 One-arm layer 3 injection — adding an injection route 61
Figure 3-38 One-arm traditional reverse proxy — topology.....62
Figure 3-39 One-arm traditional reverse proxy — configuring the default route.....63
Figure 3-40 One-arm traditional reverse proxy — adding a website.....64
Figure 3-41 Mirroring deployment topology 65
Figure 3-42 Running Mode page.....66
Figure 3-43 Mirroring mode — Work Group Management page.....66
Figure 3-44 Editing mirroring interfaces 67
Figure 3-45 New mirroring interface.....68
Figure 4-1 Active-active mode via port channel — topology 70
Figure 4-2 Active-active mode via port channel — HA configuration 71

Figure 4-3 Active-active mode via port channel — creating a work group 72
Figure 4-4 Active-active mode via OSPF — topology 73
Figure 4-5 Active-active mode via OSPF — editing interface G1/1 configuration in the work group on WAF A 75
Figure 4-6 Active-active mode via OSPF — editing interface G1/1 configuration in the work group on WAF B 75
Figure 4-7 Master/Slave mode — topology 77
Figure 4-8 Master/Slave mode — adding a work group 78
Figure 4-9 Master/Slave mode — HA configuration on the master WAF 79
Figure 4-10 Master/Slave mode — HA configuration on the standby WAF 80
Figure 5-1 Deployment of WAFs in reverse proxy mode (a single VRRP group) 83
Figure 5-2 Configuring working interface G1/1 84
Figure 5-3 VRRP Configuration page 84
Figure 5-4 Adding interface G1/1 84
Figure 5-5 VRRP Configuration page after interface G1/1 is added 85
Figure 5-6 G1/1 Instance Management page 85
Figure 5-7 G1/1 VRRP Instance Add page 86
Figure 5-8 Configuring working interface G1/2 87
Figure 5-9 VRRP Configuration page 87
Figure 5-10 Adding interface G1/2 87
Figure 5-11 VRRP Configuration page after interface G1/2 is added 88
Figure 5-12 G1/2 Instance Management page 88
Figure 5-13 G1/2 VRRP Instance Add page 89
Figure 5-14 Deployment of WAF devices in reverse proxy mode (multiple VRRP groups) 90
Figure 5-15 Creating the first VRRP instance on WAF A 91
Figure 5-16 Creating the second VRRP instance on WAF A 92
Figure 5-17 Creating the first VRRP instance on WAF B 93
Figure 5-18 Creating the second VRRP instance on WAF B 94

Preface

Scope

This document mainly describes deployment modes of NSFOCUS Web Application Firewall (WAF) V6.0 and details bypass deployment modes.

The product information involved in this document may slightly differ from your product to be installed because of version upgrades or other reasons.

Audience

This document is intended for the following users:

- Users who wish to know main features and usage of this product.
- System administrator.
- Network administrator.

This document assumes that you have knowledge of the following areas:

- Network security
- Linux and Windows operating systems
- TCP/IP protocols

Organization

Chapter	Description
1 Deployment Modes	Describes four deployment modes of WAF.
2 Deployment Principles	Describes basic principles of bypass deployment modes and the reverse proxy deployment mode.
3 Configuration Examples	Describes typical configuration examples of bypass deployment modes, the reverse proxy deployment mode, and the mirroring deployment mode.
4 HA Configuration	Describes configuration examples of the HA active-active mode and master/slave mode.
5 VRRP Configuration	Describes how to configure VRRP on WAFs.
A Default Parameters	Describes default parameters of WAF.

Conventions

Convention	Description
Bold font	Keywords, names of screen elements like buttons, drop-down lists or fields, and user-entered text appear in bold font.
Italic font	Document titles, new or emphasized terms.
A > B	Selection of menu options.
Note	Means reader take note.
Tip	Means tips for easy operation.
Caution	Means reader be careful. In this situation, you might take an action that could result in equipment damage or loss of data.
Warning	Means reader be warned. In this situation, you might take an action that could result in body injury.

Customer Support

Email: support@nsfocusglobal.com

Portal: https://nsfocus.desk.com/

Contacts:

- USA: +1-844-673-6287 or +1-844-NSFOCUS
- UK: +44 808 164 0673 or +44 808 164 0NSF
- Australia: +61 2 8599 0673 or +61 2 8599 0NSF
- Netherlands: +31 85 208 2673 or +31 85 208 2NSF
- Brazil: +55 13 4042 1673 or +55 13 4042 1NSF
- Japan: +81 3-4510-8673 or +81 3-4510-8NSF
- Singapore: +65 3158 3757
- Hong Kong +852 5803 2673 or +852 5803 2NSF
- Middle East: +973 1619 7607

1 Deployment Modes

WAF can be deployed in the following ways based on its working mode in the network:

- In-path mode
- Out-of-path mode
- Reverse proxy mode
- Mirroring mode

1.1 In-Path Deployment

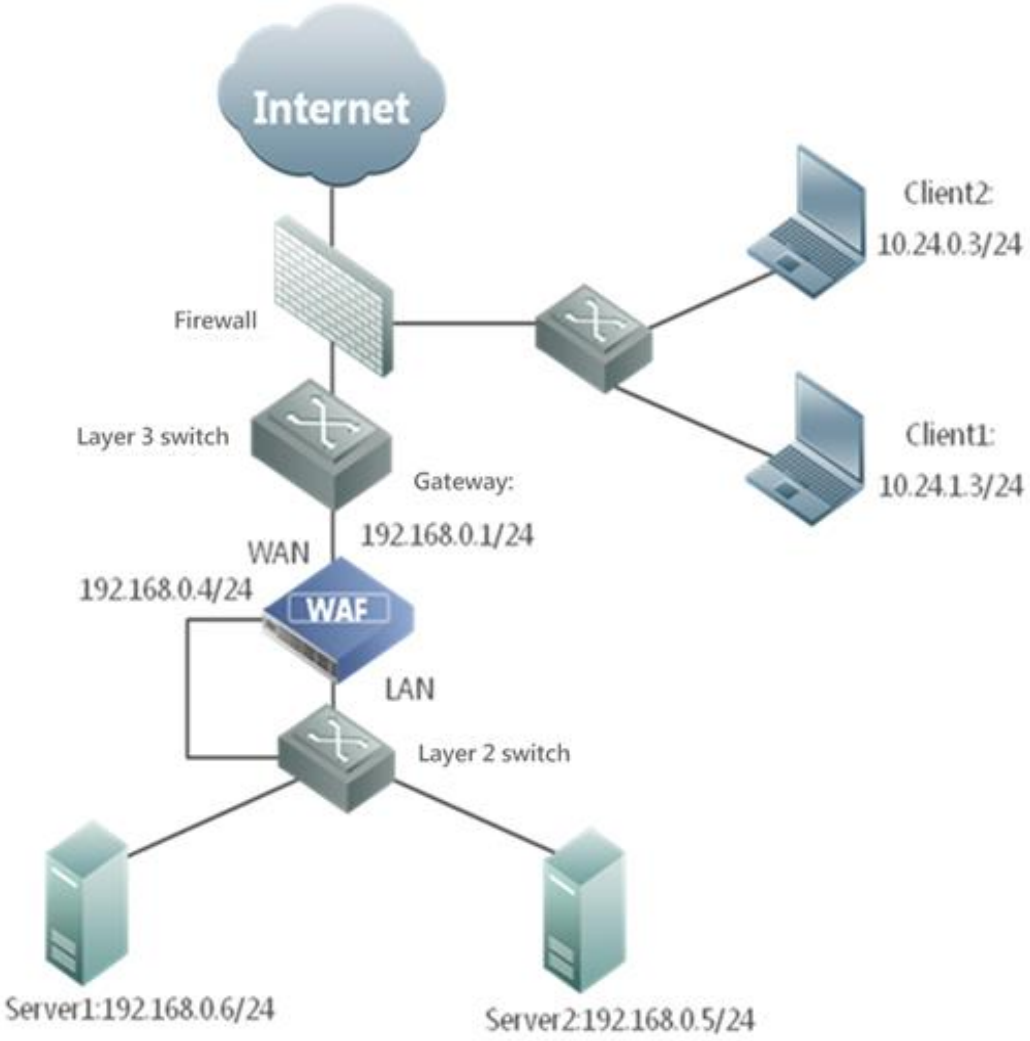
The in-path deployment mode is implemented in two ways: out-of-band management and in-band management. This mode features simple configuration and requires no major network adjustments, but problems on WAF may affect the customer's network.

Note	When configuring interfaces on WAF, note the following: • Configure the IP address of the LAN interface prior to enabling the anti-defacement function and performing scanning protection. • IP addresses in the same network segment cannot be configured for different interfaces on the same WAF.

1.1.1 In-Path Deployment with Out-of-Band Management

In this mode, the out-of-band management interface of WAF is connected to a device (usually, switch or router) on the same side as the WAN or LAN interface of WAF. Figure 1-1 shows the out-of-band management topology.

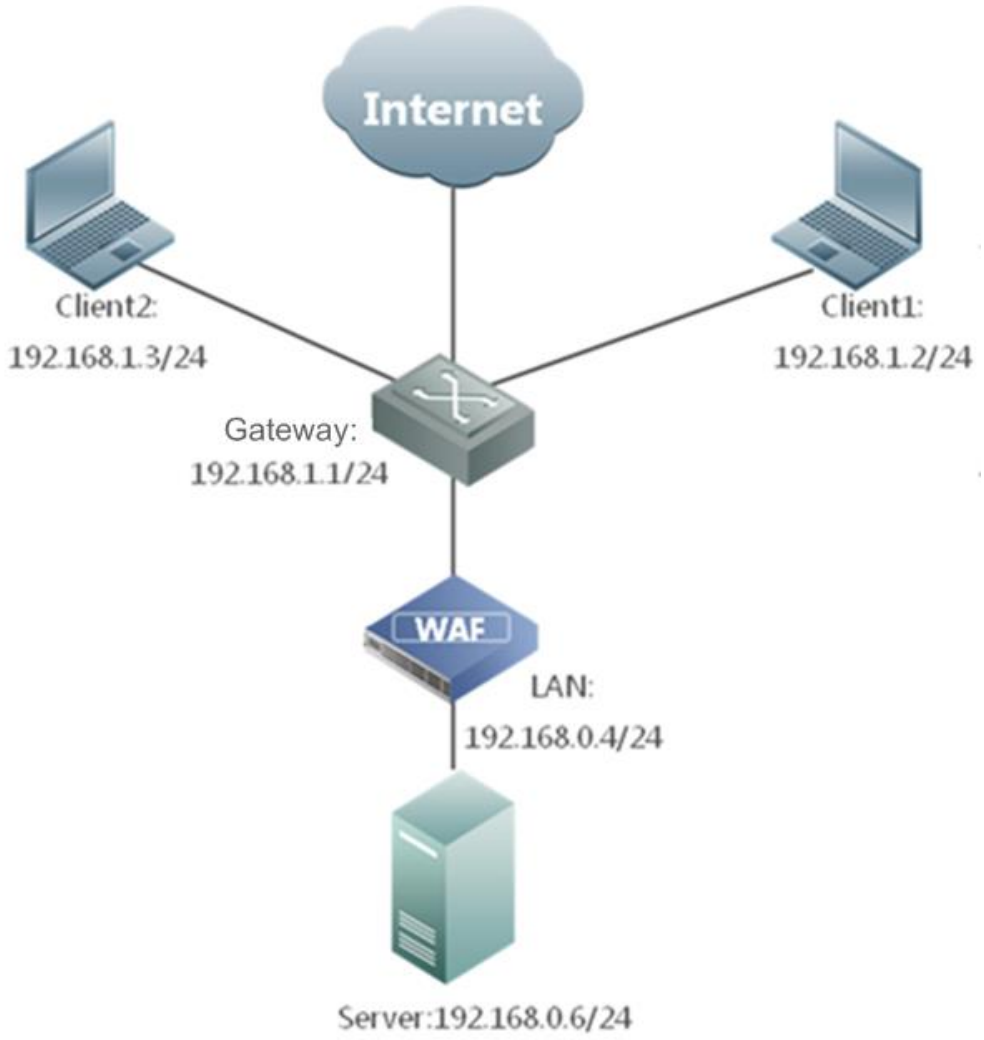
Figure 1-1 In-Path deployment — out-of-band management topology



1.1.2 In-Path Deployment with In-Band Management

In this mode, a WAN interface or LAN interface is configured as the management interface of WAF, and its IP address is managed from the same side of the WAN or LAN interface. Figure 1-2 shows the in-band management deployment topology.

Figure 1-2 In-Path Deployment — in-band management topology



1.2 Out-of-Path Deployment

In out-of-path deployment mode, WAF, connected to the network in an out-of-path way, diverts traffic destined for the server for cleaning, and then injects the processed traffic back to the network. Responses from the server are forwarded by WAF to the client. In this mode, WAF is physically deployed in an out-of-path way, while logically all bidirectional traffic between the web server and clients passes through WAF. Figure 1-3 shows the deployment topology.

The major advantages of out-of-path deployment are as follows:

- WAF can detect and handle traffic only destined to the server to be protected.
- If WAF fails or reaches the upper performance limit, in the worst situation, it only affects the traffic passing through WAF, but has no impact on other systems or applications in the network.

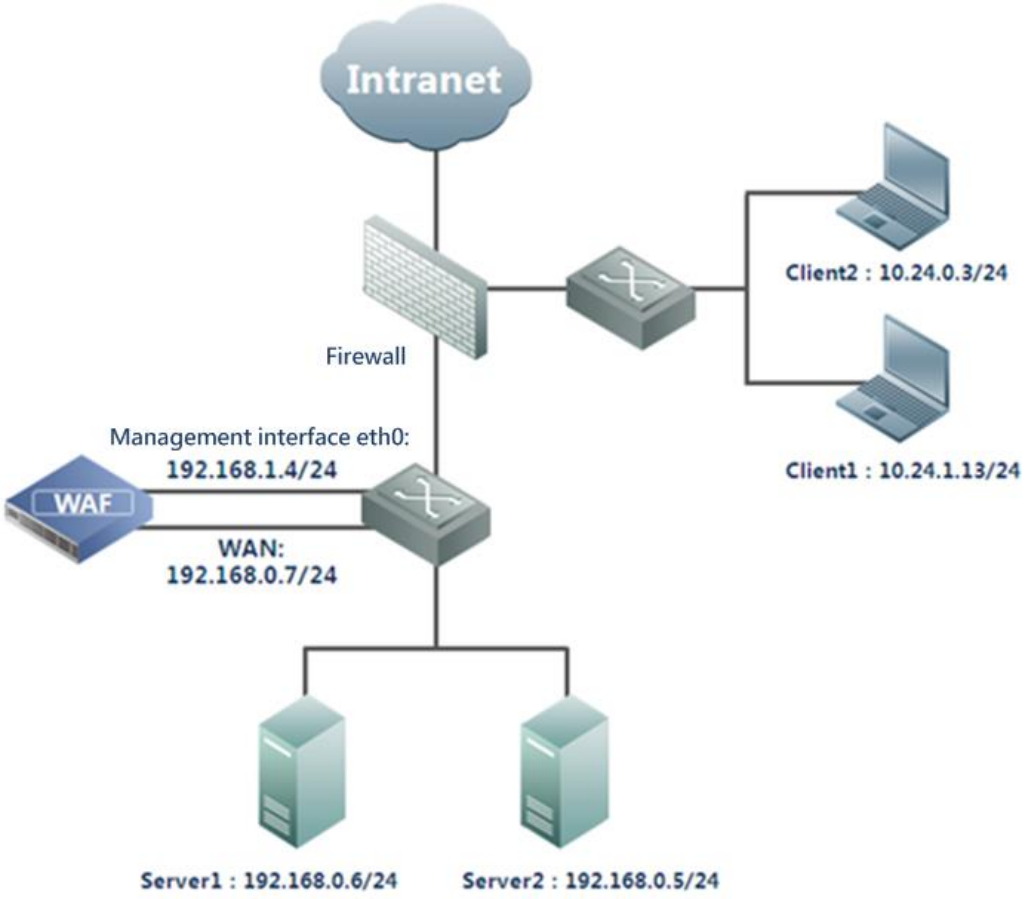
In out-of-path deployment mode, WAF is transparent to clients. Therefore, this mode is also known as the semi-transparent proxy mode. WAF is transparent to the clients. The routing device diverts the request traffic to WAF by modifying the route to the destination

server, while it appears to client-side devices (client hosts and firewall residing before WAF) that requests destined for the server are still using the IP address and port of the destination server.

For the server side, however, WAF works as the proxy in this mode. To ensure that HTTP responses pass through WAF, WAF changes the source IP address of the received requests to the IP address of its own working interface. Therefore, it seems to server-side devices (server and firewall residing behind WAF) that all requests come from the IP address of the working interface on WAF.

WAF, like a standard proxy server, uses the "X-Forwarded-For" field in the HTTP header to identify the actual source IP address (client IP address) of requests and indicate it to web services and web applications.

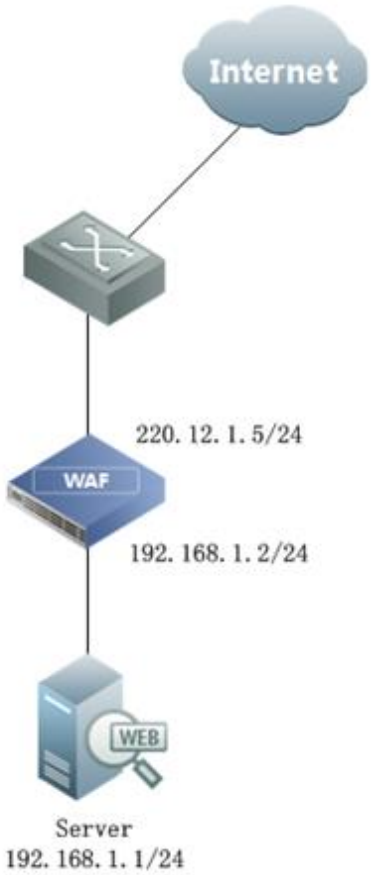
Figure 1-3 Out-of-path deployment topology



1.3 Reverse Proxy Mode

In reverse proxy mode, WAF is deployed in front of the server to receive connection requests from Internet clients, apply policies to them, and pass compliant requests to the server. Also, WAF forwards the server's responses to Internet clients. To Internet clients, WAF acts as the server. Figure 1-4 shows the deployment topology.

Figure 1-4 Reverse proxy deployment topology



In this mode, the client sends requests to WAF, and then WAF handles the requests and passes them to the server. Therefore, the server views WAF as the source of requests. In other words, both the client and server are invisible to each other in this mode.

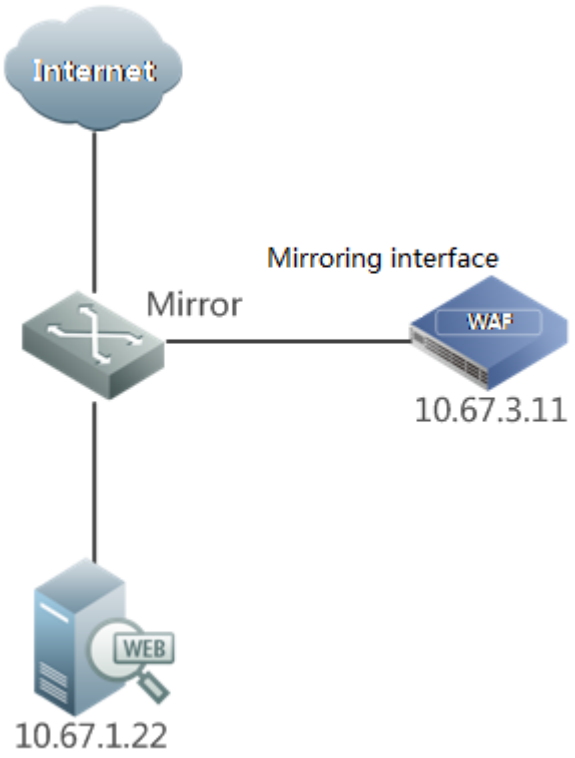
In this mode, WAF forwards only HTTP traffic that matches its policies, and drops mismatched traffic.

WAF, like a standard proxy server, uses the "X-Forwarded-For" field in the HTTP header to identify the actual source IP address (client IP address) of requests and indicate it to web services and web applications.

1.4 Mirroring Deployment

In mirroring deployment mode, WAF connects to the switch via a mirroring interface. After WAF and the switch are configured accordingly, the traffic passing through the web server can be mirrored to WAF with the mirroring interface for analysis and detection. Figure 1-5 shows the deployment topology.

Figure 1-5 Mirroring deployment topology



The traffic can be mirrored in one of the following ways:

- Configure the switch to mirror the uplink and downlink traffic of the LAN interface to the mirroring interface, which directly connects to the mirroring interface of WAF with a network cable.
- Configure the switch to mirror the uplink and downlink traffic of the WAN interface to the mirroring interface, which directly connects to the mirroring interface of WAF with a network cable.
- Configure the switch to mirror the uplink traffic of the LAN interface and the downlink traffic of the WAN interface to the mirroring interface, which directly connects to the mirroring interface of WAF with a network cable.

1.5 Comparison Among Deployment Modes

Deployment Mode	Strength	Weakness
In-path deployment	• Easy deployment. • No major changes to the customer's network.	The customer's network is not immune to problems on WAF. All traffic in the network passes through WAF, greatly increasing the load on WAF.

Deployment Mode	Strength	Weakness
Out-of-path deployment	• High resource utilization as WAF only handles traffic of the web server. • No single point of failures (SPOFs).	The deployment is complex as it requires configurations of layer 2 or layer 3 traffic diversion.
Reverse proxy	• Easy deployment. • High resource utilization as WAF only handles HTTP traffic. • No SPOFs.	This deployment mode brings great impacts on the customer's business logic as certain information needs to be changed, including the customer's public IP address, server IP address, and DNS parsing configurations. The server side and client side are invisible to each other.
Mirroring	• No changes to the customer's network topology. • No impact on customer services. • Big throughput.	In this mode, WAF only detects attacks against customer's business, without provide protection.

2 Deployment Principles

This chapter describes the principles for out-of-path and one-arm reverse proxy deployment.

2.1 Out-of-Path Deployment

This section describes principles of traffic diversion and injection in out-of-path deployment mode:

- Traffic Diversion
- Layer 2 Injection
- Crossover Injection
- PBR Injection

2.1.1 Traffic Diversion

Traffic diversion here means to divert the traffic destined for a protected server to WAF for processing. To achieve this purpose, you need to configure a high-priority route on the router or switch that is directly connected to WAF. Based on the longest prefix matching principle, the high-priority route needs to be a static route that ends at the IP address of the target server and uses the IP address of a working interface of WAF as the next-hop IP address.

2.1.2 Layer 2 Injection

Assume the following scenario:

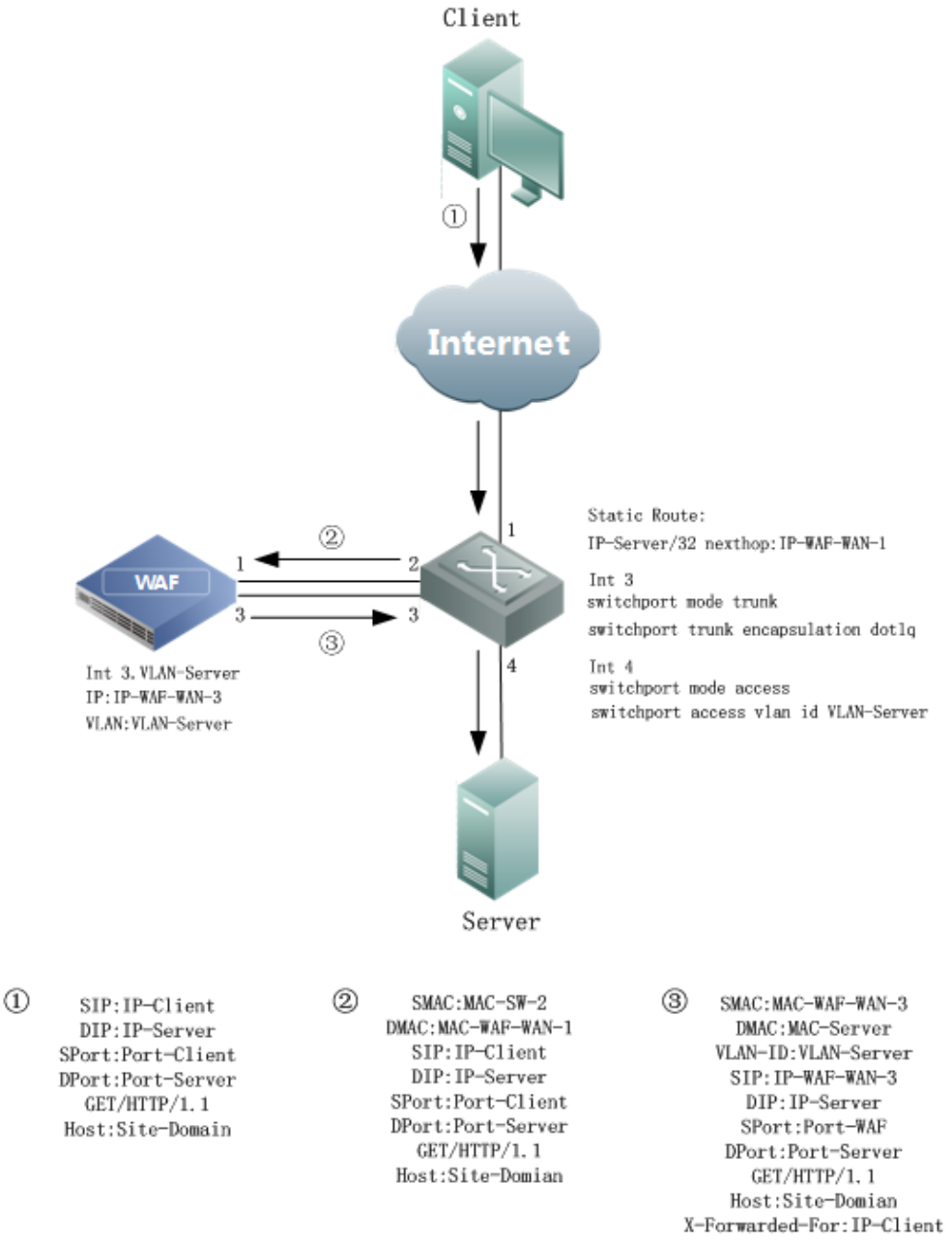
1. The diversion interface and injection interface on WAF are connected to the same layer 3 switch.
2. The layer 3 switch connects to the server via an interface that belongs to a specific VLAN or is configured as a trunk interface encapsulated with dot1q.

If the layer 3 switch acts as the server gateway, it fails to specify the next-hop IP address for injected traffic via PBR. To solve this problem, the switch sends the traffic to the target server via the layer 2 forwarding mechanism, that is, it sends injected traffic to the broadcast domain to which the target server belongs, using the MAC address of the NIC of the target server as the target MAC address of packets.

Downlink Traffic

Figure 2-1 shows the forwarding paths and packet header changes of downlink traffic (client-to-server requests) during diversion and PBR injection.

Figure 2-1 Layer 2 injection — downlink traffic



The trunk encapsulation dot1q is enabled between interface 3 on WAF and interface 3 on the switch. Interface 3 on WAF needs to be configured with a subinterface, with the IP address of the subinterface set to an idle IP address in the network segment of the server to be protected and the dot1q value specified as the VLAN ID of this network segment. The downlink traffic is processed as follows:

1. The client sends a request to the layer 3 switch via the Internet.
2. The switch forwards the request to interface 1 on WAF for processing along the configured diversion route (32-bit static route).
3. WAF first handles the request.

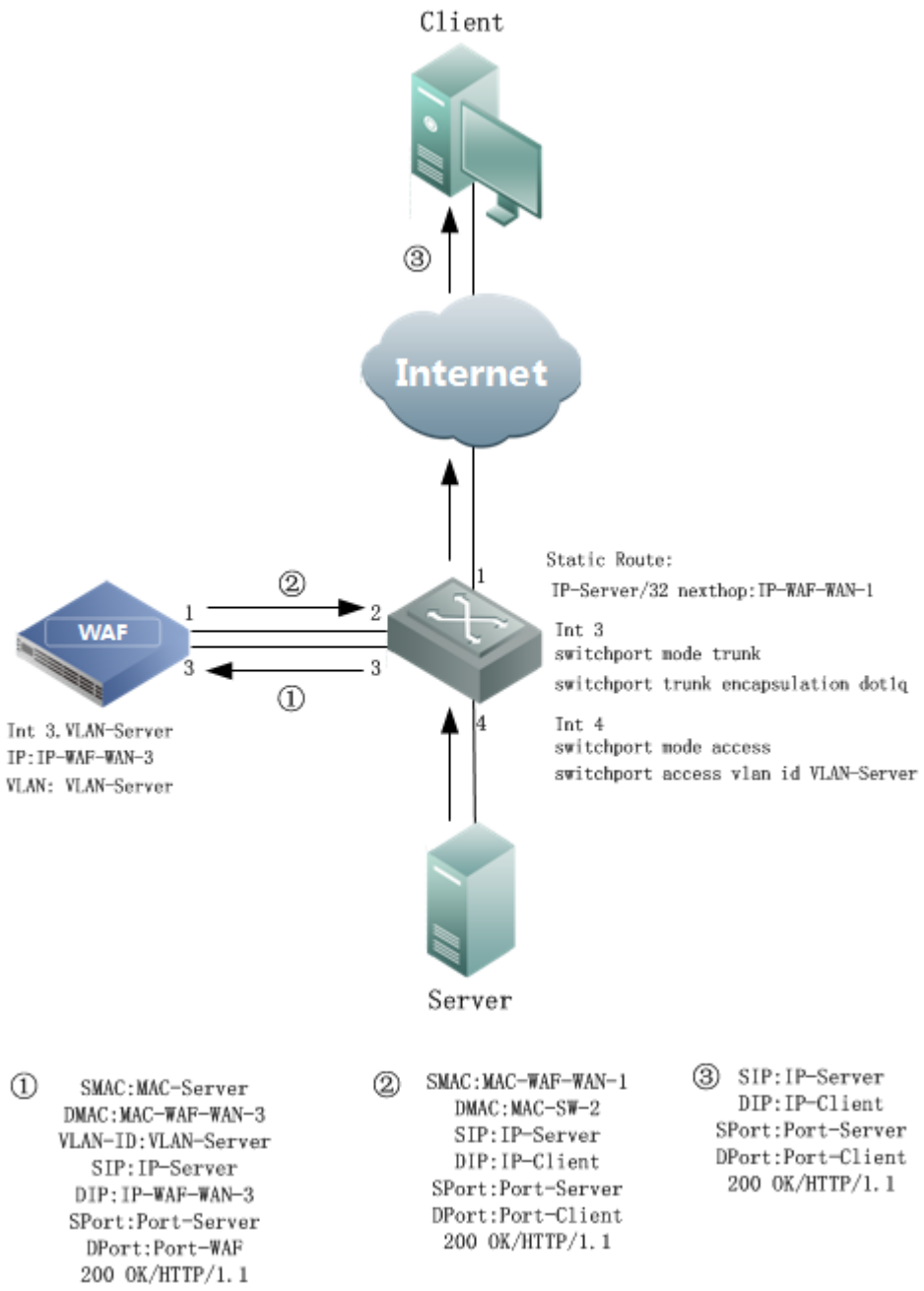
4. WAF sends the handled request to the switch. To ensure that the server's response to the handled request can reach WAF, WAF uses its own interface IP address and TCP port as the source IP address and source port of the handled request. Meanwhile, WAF records the mapping between the source information (source IP address and port) in the handled request and that in the original request. Also, WAF uses the "X-Forwarded-For" field in the HTTP header to identify the actual source IP address (client IP address) of requests and indicate it to web services and web applications. According to the interface configuration (direct route and VLAN ID), WAF encapsulates the request packet with the dot1q value set to VLAN-Server and sends the packets over interface 3, that is, using the IP address of interface 3 as the source IP address.
5. After the request arrives at interface 3 on the switch, the switch attempts to send the request via layer 2 forwarding because the destination MAC address of this request is not the MAC address of interface 3 of the switch. According to the CAM table, the switch sends the request to the server via interface 4.

Note	On the switch, you need to disable the ARP proxy function of the VLAN where the server resides. Otherwise, when WAF queries the MAC address of the server, the switch may return its own MAC address to WAF. To disable the ARP proxy function on a Cisco switch, run the following commands (replacing **<VLAN-Server>** with the actual VLAN ID of the server): **(config)# interface vlan <VLAN-Server>** **(config-if)# no ip proxy-arp**

Uplink Traffic

Figure 2-2 shows the forwarding paths and packet header changes of uplink traffic (server-to-client responses) during diversion and layer 2 injection.

Figure 2-2 Layer 2 injection — uplink traffic



The uplink traffic is handled as follows:

a. The server sends HTTP responses whose destination MAC address and destination IP address are respectively the MAC address and IP address of the injection interface on WAF.

b. After receiving HTTP responses from the server, the switch queries the CAM table for the destination IP address based on the destination MAC address and forwards responses to WAF via interface 3.

c. WAF handles the received HTTP responses and then encapsulates the handled response packets, using the IP address and the TCP port of the client as the destination IP address and destination port according to the mapping recorded previously.

d. WAF sends encapsulated response packets to the switch via the diversion interface (interface 1).

e. After querying the routing table, the switch sends the received response packets to the client via the Internet.

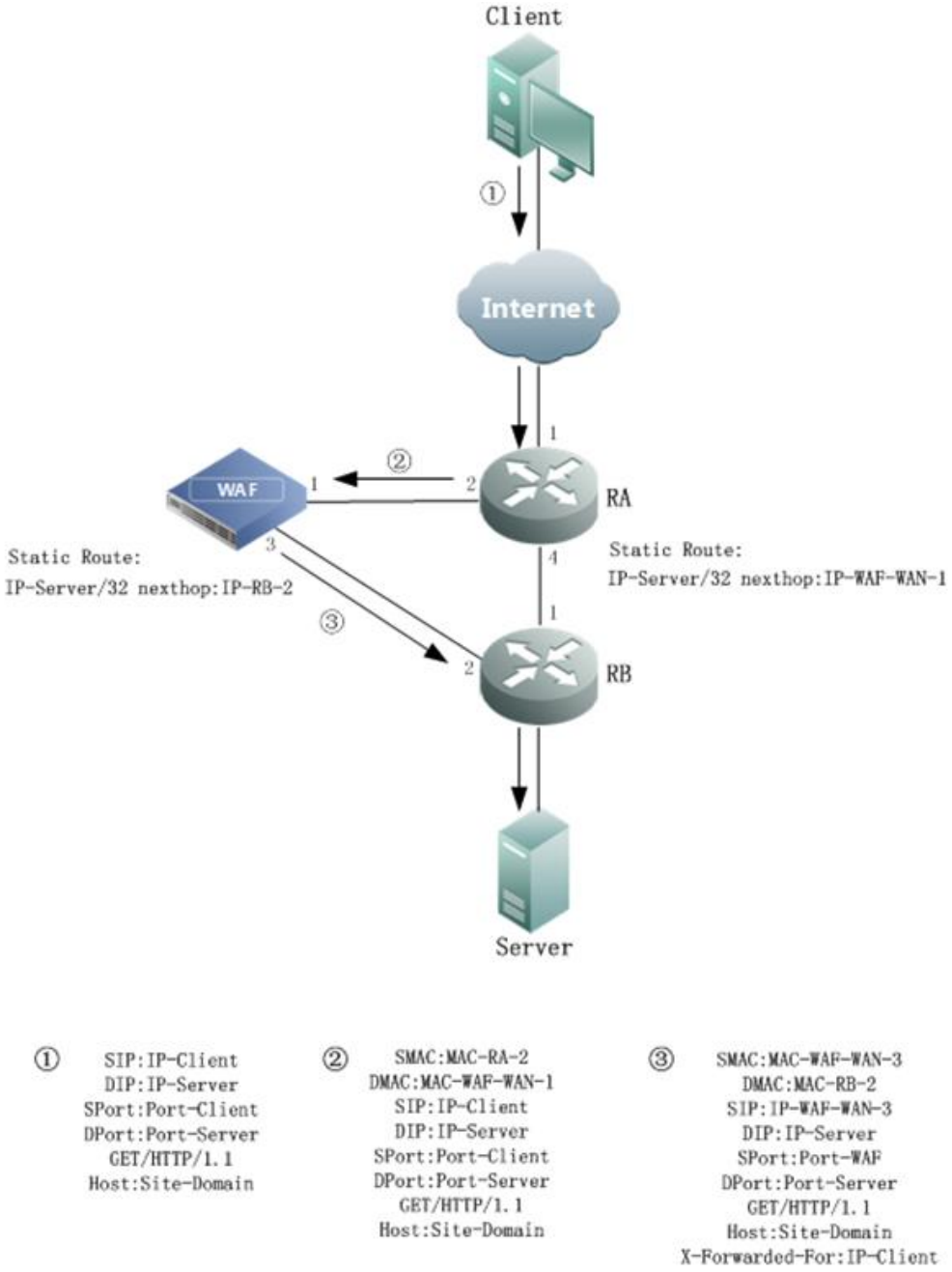
2.1.3 Crossover Injection

In crossover injection mode, the router connecting to the injection interface on WAF resides in the downlink of the router connecting to the diversion interface on WAF. As no diversion route exists in the router connecting to the injection interface on WAF, the router sends the injection traffic to the next-hop IP address along a normal route, without traffic diversion.

Downlink Traffic

Figure 2-3 shows the forwarding paths and packet header changes of downlink traffic (client-to-server requests) during diversion and crossover injection.

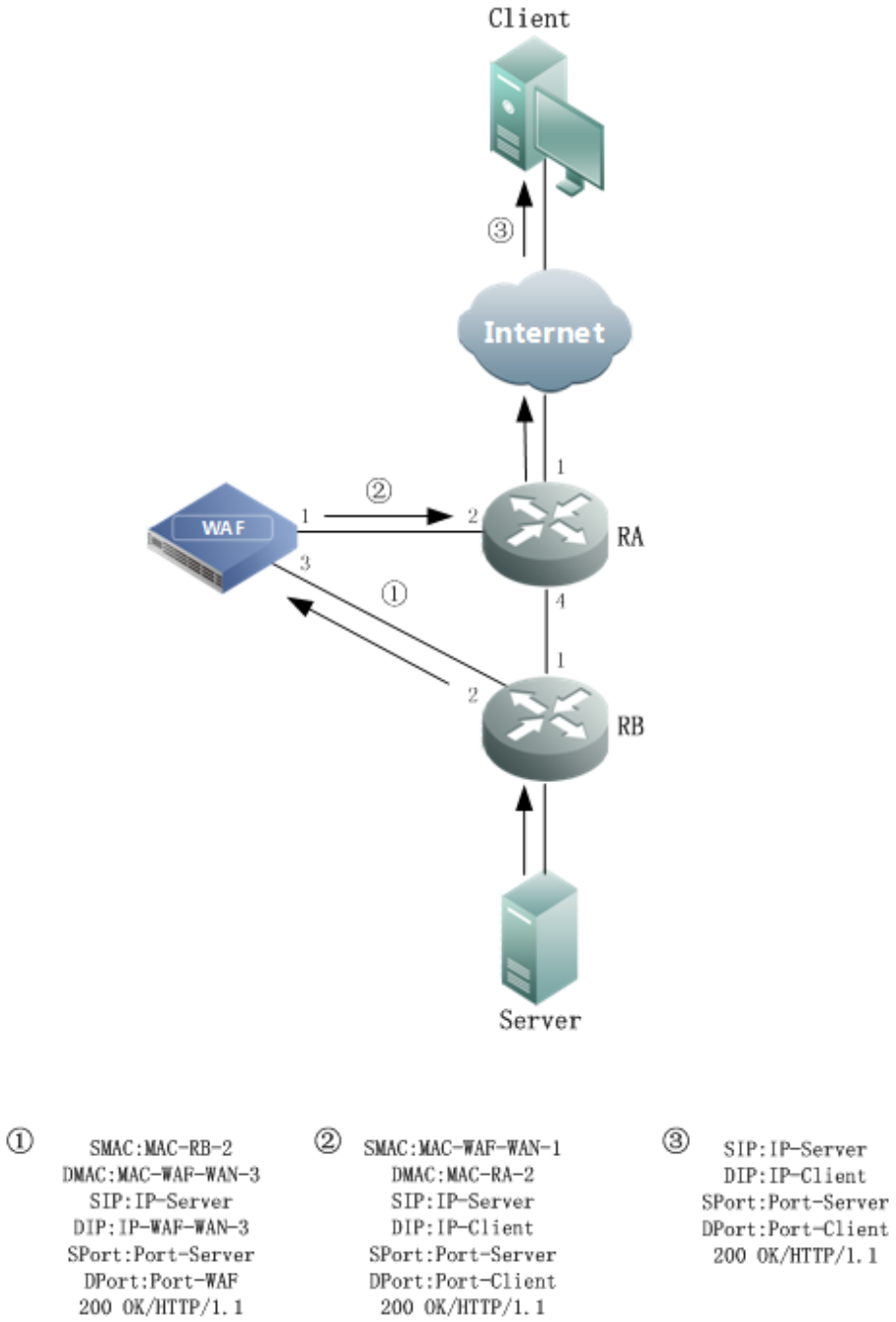
Figure 2-3 Crossover injection — downlink traffic



Uplink Traffic

Figure 2-4 shows the forwarding paths and packet header changes of uplink traffic (server-to-client responses) during diversion and crossover injection.

Figure 2-4 Crossover injection — uplink traffic



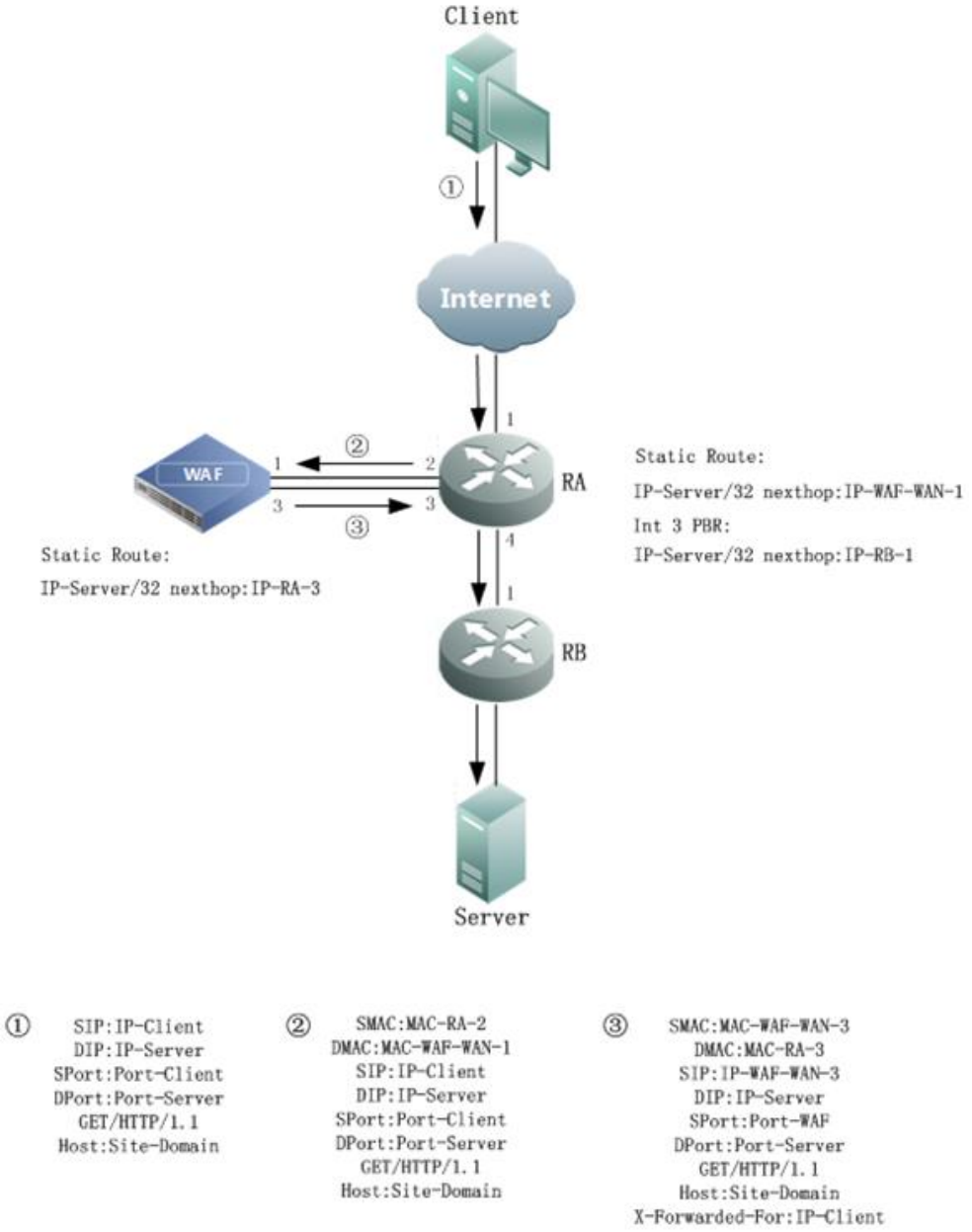
2.1.4 PBR Injection

Assume that the injection interface and diversion interface on WAF connect to the same router. In this case, if the gateway exists between the router and the server, you need to configure a policy-based route (PBR) on the injection interface of the router. As the interface-based PBR has a higher priority than global routes (in the routing table including the diversion route), the router forwards injection traffic along the PBR to the proper next-hop IP address. This avoids a routing loop due to injection traffic diversion by the router.

Downlink Traffic

Figure 2-5 shows the forwarding paths and packet header changes of downlink traffic (client-to-server requests) during diversion and PBR injection.

Figure 2-5 PBR injection — downlink traffic



In the preceding topology, interface 1 on WAF and interface 2 on Router A are in the same network segment; interface 3 on WAF is in the same network segment as interface 3 on Router A. The downlink traffic is processed as follows:

1. The client sends a request to Router A via the Internet.
2. Router A forwards the request along the configured diversion route (32-bit static route) to interface 1 on WAF for processing.

3. WAF handles this request. To ensure that the server's response to the handled request can reach WAF, WAF uses the IP address of its injection interface (interface 3) and its TCP port as the source IP address and source port of requests when sending the handled request to the server. Meanwhile, WAF records the mapping between the source information (source IP address and port) in the handled request and that in the original request. Also, WAF uses the "X-Forwarded-For" field in the HTTP header to identify the actual source IP address (client IP address) of requests and indicate it to web services and web applications.
4. WAF, along the configured static route, sends the injection traffic via its interface 3 to interface 3 on Router A.
5. Router A, along the configured PBR, forwards the traffic via interface 3 to interface 1 on Router B.
6. After receiving the injection traffic, Router B forwards it to the server.

Note	• The diversion interface and injection interface on WAF should come from different bypass interface pairs. • If WAF is directly connected to a layer 3 switch, you are advised to configure the diversion interface of the switch as a layer 3 interface. The following is the configuration command for a Cisco switch: **(config)# interface GigabitEthernet0/2** **(config-if)# no switchport**

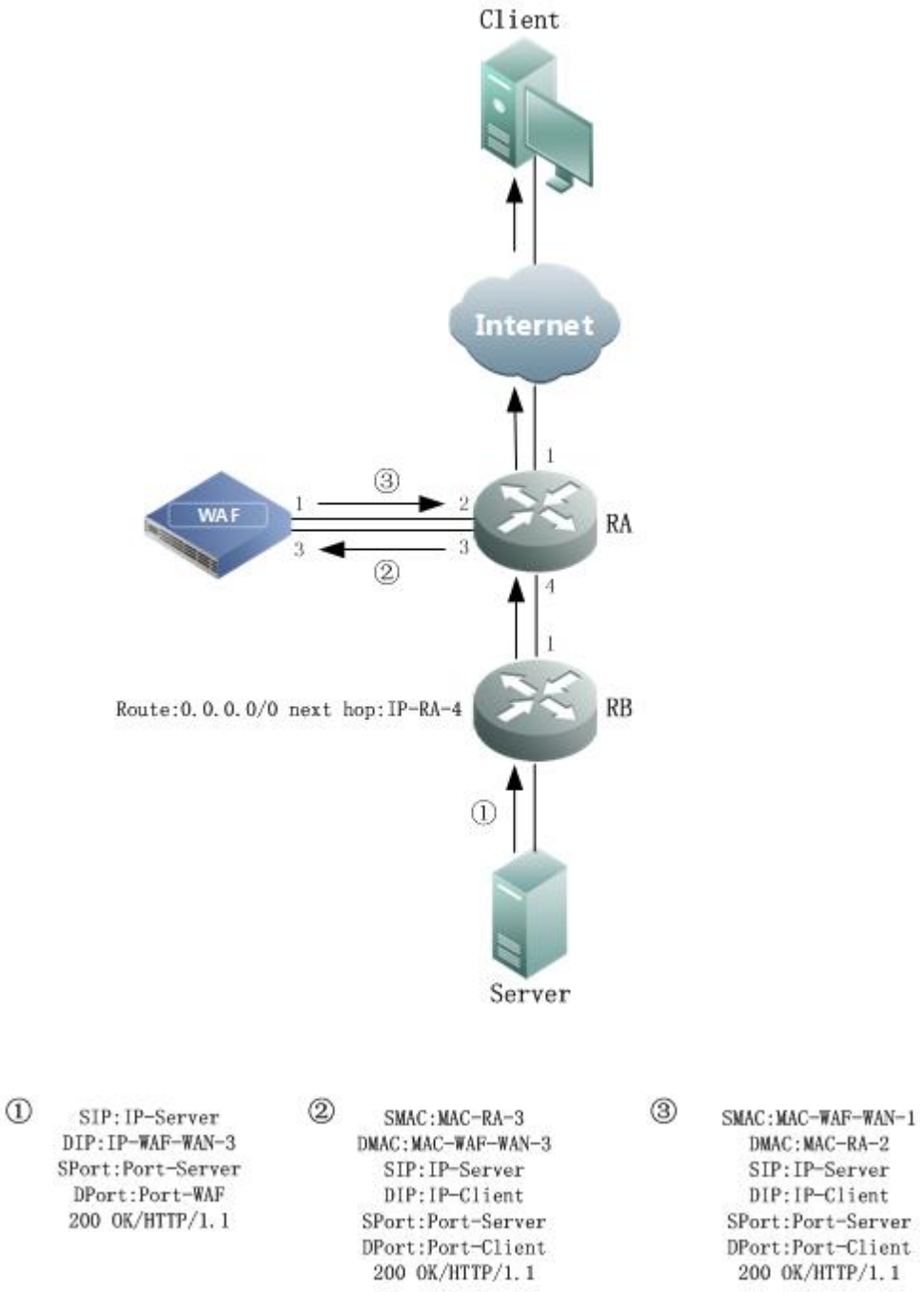
Traffic diversion and injection can also be achieved in one-arm mode:

- WAF connects to a router in one-arm mode. In this case, traffic diversion and injection can be achieved via one or two pairs of interconnected IP addresses. If two pairs of interconnected IP addresses are used, you need to configure subinterfaces on the router interface.
- WAF connects to a layer 3 switch. As most interfaces of a layer 3 switch do not support subinterfaces, you are advised to use one pair of interconnected IP addresses to achieve diversion and injection.

Uplink Traffic

Figure 2-6 shows the forwarding paths and packet header changes of uplink traffic (server-to-client responses) during diversion and PBR injection.

Figure 2-6 PBR injection — uplink traffic



The uplink traffic is handled as follows:

a. The server sends an HTTP response, with the destination IP address being the IP address of the injection interface of WAF.

b. After receiving the response from the server, Router B forwards it to Router A along the default route to Router A, instead of the route to the injection interface of WAF.

c. Router A forwards the response to the injection interface (interface 3) on WAF along a direct route.

d. WAF first handles the received response and then encapsulates the response, using the IP address and the TCP port of the client as the destination IP address and destination port according to the correspondence recorded previously.

e. WAF sends the encapsulated response packet to Router A via the diversion interface (interface 1).

f. After querying the routing table, Router A sends the received response packet to the client via the Internet.

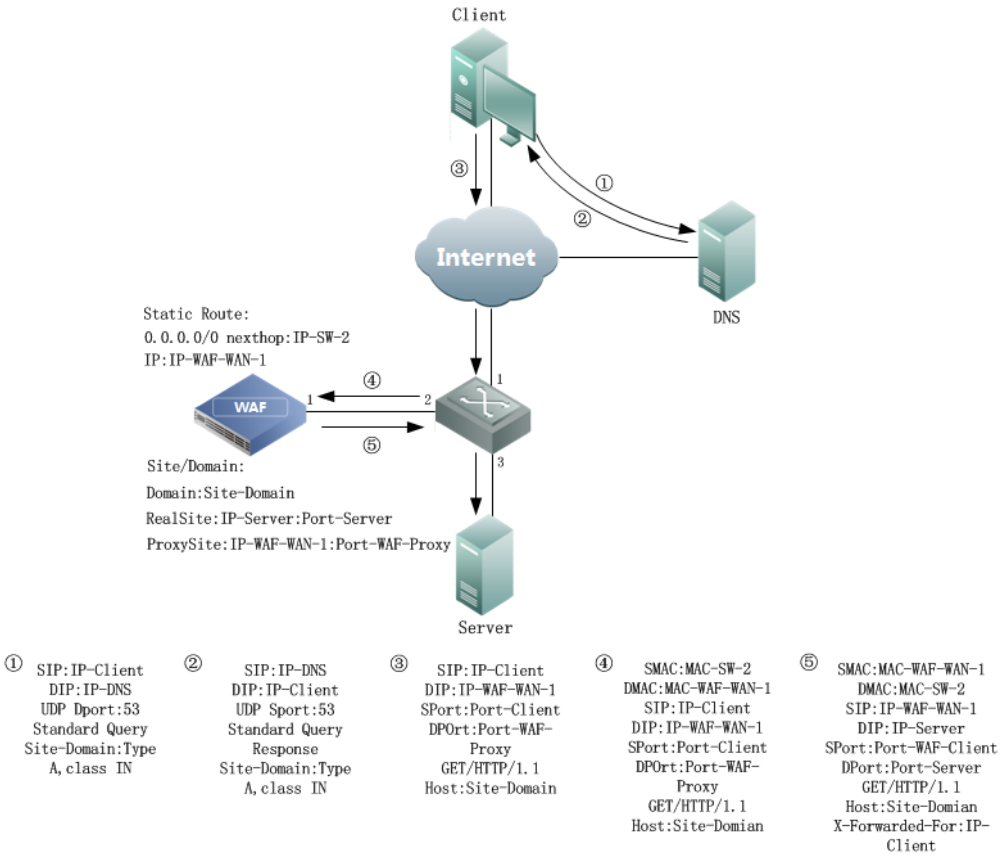
2.2 One-Arm Reverse Proxy Deployment

The reverse proxy deployment mode applies if you would rather change the DNS parsing configuration or the IP address of the server than alter the router configuration when deploying WAF. To minimize changes to your network, you can employ the flexible one-arm reverse proxy deployment mode in which WAF is deployed like a reverse proxy server.

Downlink Traffic

Figure 2-7 shows the forwarding paths and packet header changes of downlink traffic (client-to-server requests) in one-arm reverse proxy mode.

Figure 2-7 One-arm reverse proxy mode — downlink traffic



The downlink traffic is handled as follows:

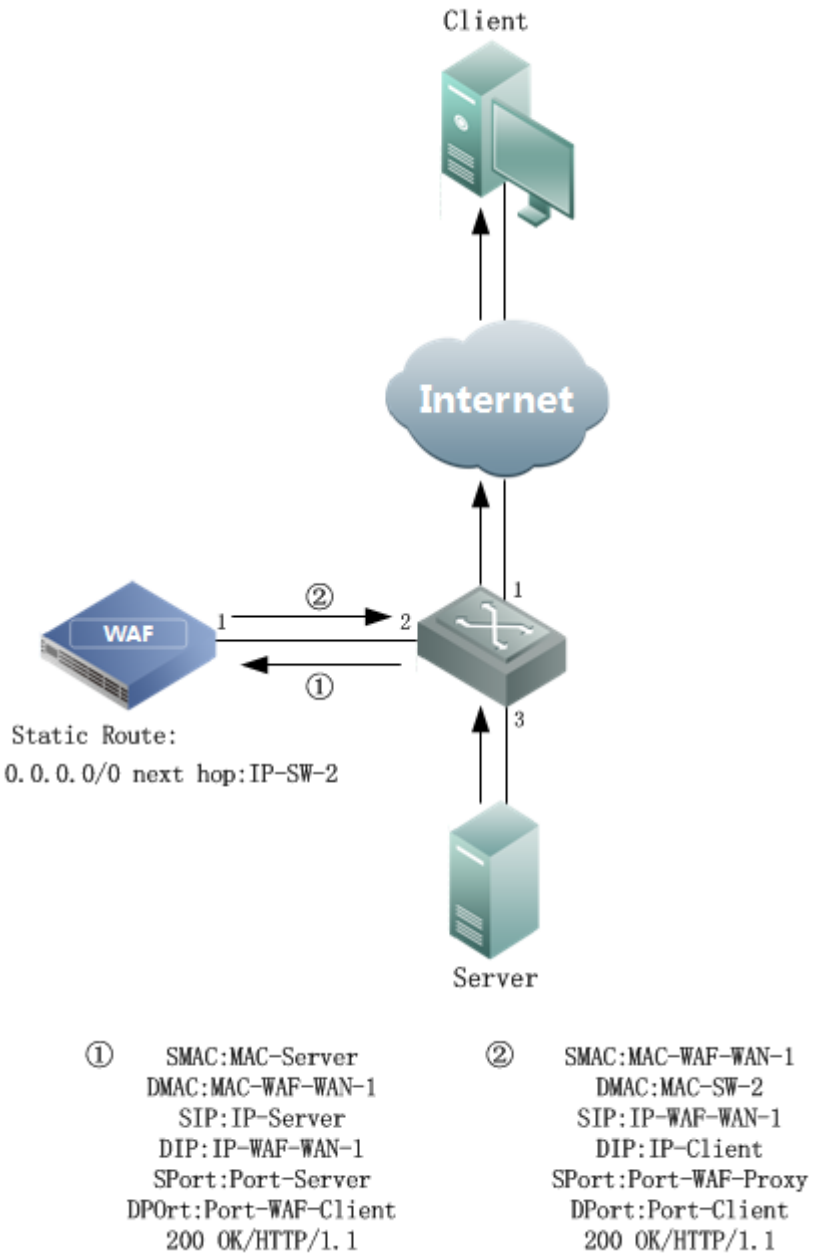
1. The client queries the DNS server for the domain name of the website.
2. The DNS server returns the client the IP address of WAN-1 interface as the IP address of the site.
3. The client establishes TCP connections with the IP address (proxied IP address) of WAN-1 interface on WAF and service port (proxied port) and sends an HTTP request. In this phase, WAF appears as a web server.
4. WAF handles the HTTP request from the client.
5. WAF sends the HTTP request, using the IP address of WAN-1 interface and its port as the source IP address and source port. Also, WAF records the mapping between the source information (source IP address and port) in the handled request and that in the original request.
6. WAF uses the "X-Forwarded-For" field in the HTTP header to identify the actual source IP address (client IP address) of requests and indicate it to web services and web applications.

Caution	• WAF needs to be configured with a correct default route (the next hop is the IP address of interface 2 on the switch) to the client and server. Otherwise, WAF may fail to properly communicate with the client or server. • In the preceding deployment example, you need to modify DNS parsing configuration, that is, changing the website's IP address to WAF's IP address when the client accesses the website or changing the server's IP address, and configuring WAF with the original IP address of the server.

Uplink Traffic

Figure 2-8 shows the forwarding paths and packet header changes of uplink traffic (server-to-client responses) in one-arm reverse proxy mode.

Figure 2-8 One-arm reverse proxy mode — uplink traffic



The uplink traffic is handled as follows:

1. The server sends an HTTP response to the WAN-1 interface of WAF.
2. WAF handles the received HTTP response.
3. Based on the mapping between the original request and proxied request, WAF sends the handled response, using the IP address (proxied IP address) of the WAN-1 interface and its service port (proxied port) as the source IP address and source port.

3 Configuration Examples

This chapter describes configuration examples for out-of-path, one-arm reverse proxy deployment, and mirroring deployment.

Note	• Switches in all configuration examples in this chapter refer to Cisco 3750 series switches. • WAF V6.0R04F00 and later support both IPv4 and IPv6 deployment. This chapter uses IPv4 as examples. To perform IPv6 deployment, add IPv6-related configurations. • The default management interface is M or H1, and working interface names are in the format of G plus interface board number/interface number, for example G1/1 and G1/2.

3.1 Out-of-Path Deployment

This section presents configuration examples of the following out-of-path deployment modes:

- Diversion via Static Route
- Layer 2 Injection
- Crossover Injection
- PBR Injection

3.1.1 Diversion via Static Route

Configure a static route from the switch directly to a working interface on WAF.

Switch Configuration

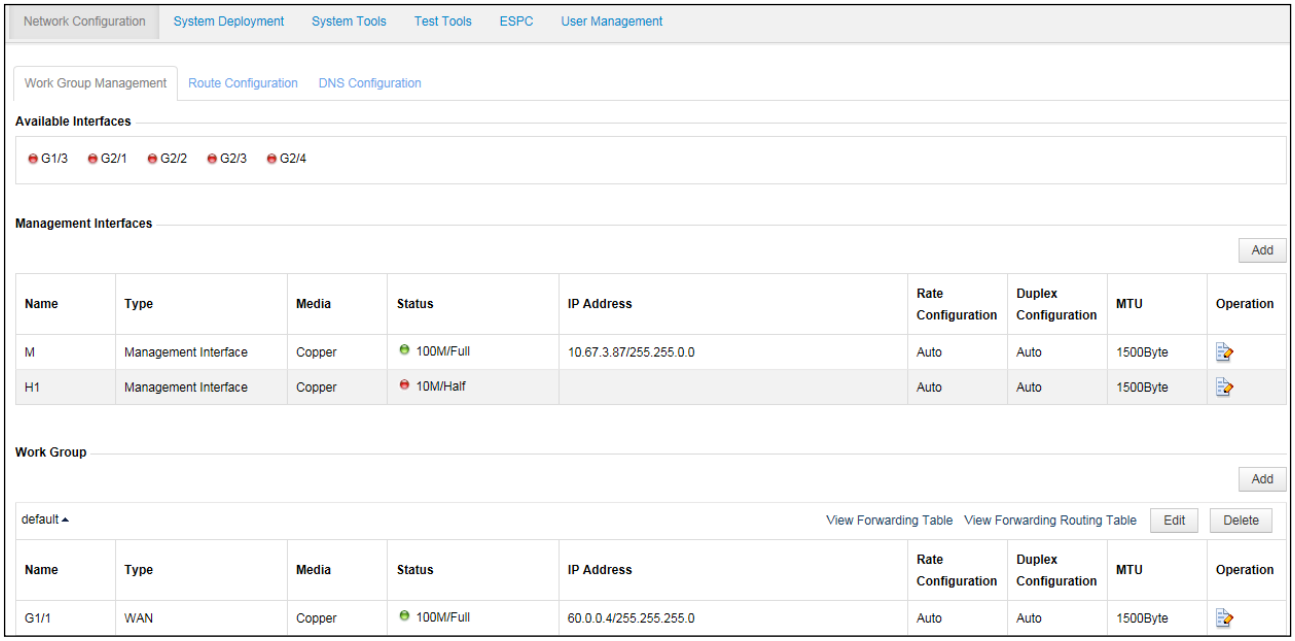
Configuration Command	Description
#interface GigabitEthernet 0/1 # ip address 3.3.3.2 255.255.255.252 # no shutdown #ip route 1.1.1.10 255.255.255.255 3.3.3.1	These commands configure a static route from the switch directly to a working interface on WAF.

WAF Configuration

Perform the following operations to change the IP address of a working interface of WAF:

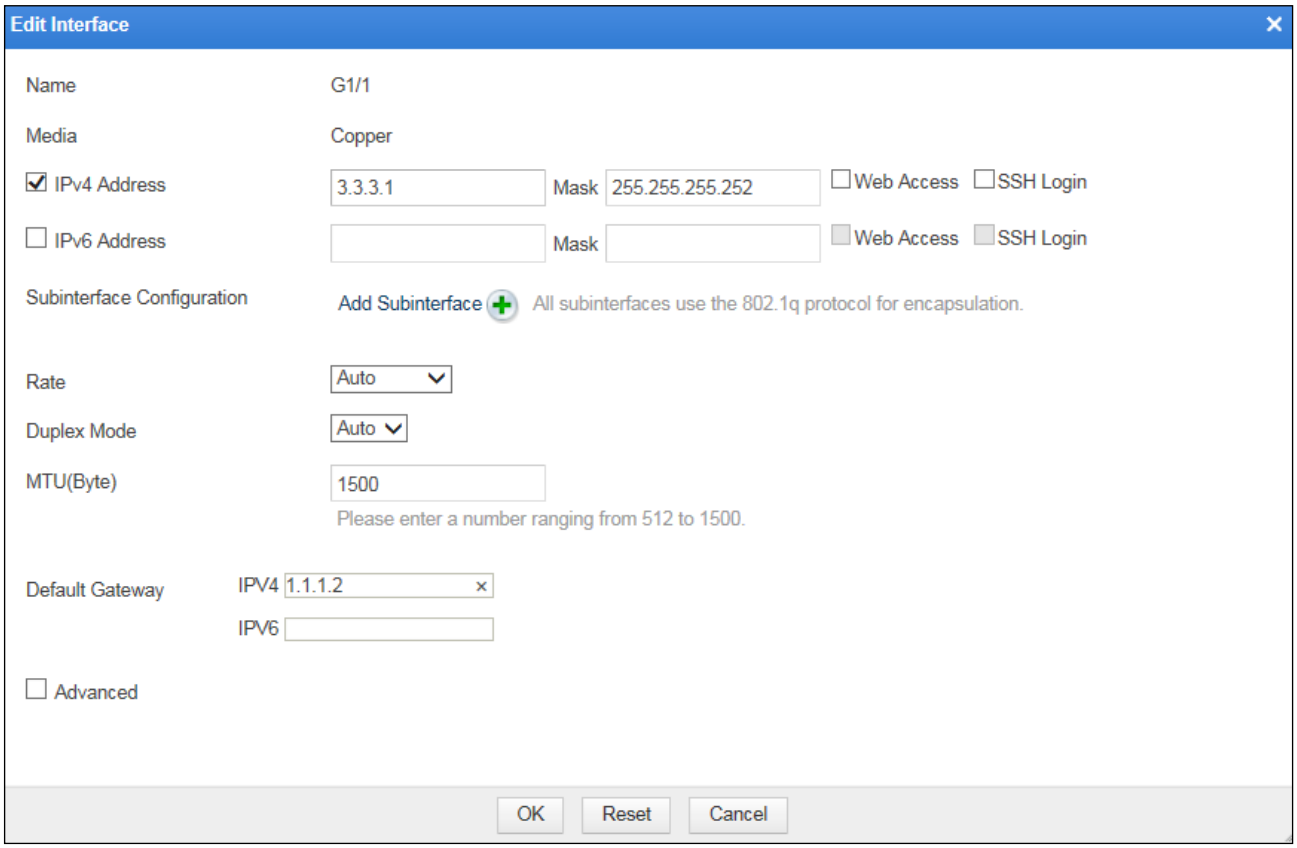
Step 1 Choose **System Management > Network Configuration > Work Group Management**.

Figure 3-1 Diversion via static route — Work Group Management page



Step 2 Click in the row of interface **G1/1** in the **default** group and edit interface parameters in the **Edit Interface** dialog box, as shown in Figure 3-2.

Figure 3-2 Diversion via static route — editing interface G1/4 configuration



Step 3 Click **OK** to complete the configuration.

Run the following command on the switch to check whether the configuration takes effect:

```
#show ip route 1.1.1.10
Routing entry for 1.1.1.10/32
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 3.3.3.1
      Route metric is 0, traffic share count is 1
```

The command output shows that only one route entry involves the IP address of interface G1/1 on WAF.

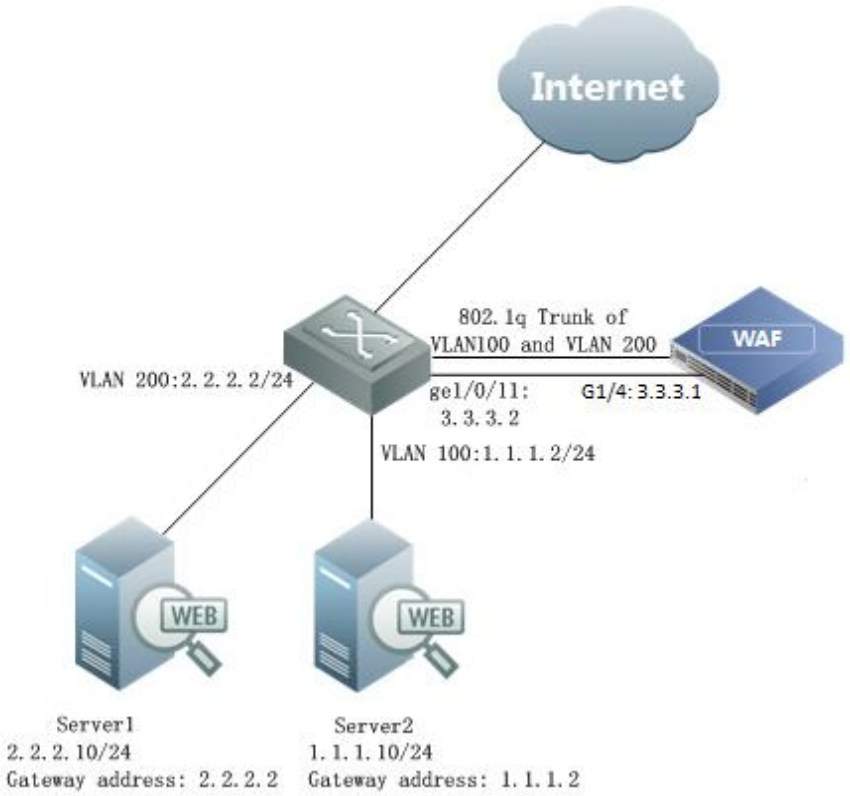
----End

3.1.2 Layer 2 Injection

Scenario

WAF protects multiple VLANs simultaneously and proxies the access to two servers, 1.1.1.10 and 2.2.2.10. Therefore, for the server 1.1.1.10, access requests appear to come from the IP address (1.1.1.1) of VLAN 100 on WAF; for the server 2.2.2.10, access requests seem to come from the IP address (2.2.2.1) of VLAN 200 on WAF. WAF uses interface G1/4 as the diversion interface and uses interface G1/2 as the injection interface. Figure 3-3 shows the topology.

Figure 3-3 Layer 2 injection — topology



Switch Configuration

Configuration Command	Description
interface GigabitEthernet1/0/11 description Connect-To-WAF-Diversion no switchport ip address 3.3.3.2 255.255.255.252 !	These commands configure the diversion interface as a layer 3 interface that directly connects to interface G1/4 on WAF.
interface GigabitEthernet1/0/13 switchport trunk encapsulation dot1q switchport trunk allowed vlan 100,200 switchport mode trunk !	These commands configure an injection interface that: • Directly connects to interface G1/2 on WAF. • Works in trunk mode and uses dot1q encapsulation. • Allows traffic from VLAN 200 to pass through.
interface GigabitEthernet1/0/15 switchport access vlan 200 switchport mode access !	These commands configure the interface used by the switch to connect to server 1.

Configuration Command	Description
interface GigabitEthernet1/0/21 switchport access vlan 100 switchport mode access !	These commands configure the interface used by the switch to connect to server 2.
interface Vlan100 ip address 1.1.1.2 255.255.255.0 no ip proxy-arp !	These commands achieve the following: • Configure VLAN 100 to which server 2 belongs and the IP address of server 2. • Disable proxy ARP in VLAN 100.
interface Vlan200 ip address 2.2.2.2 255.255.255.0 no ip proxy-arp	These commands achieve the following: • Configure VLAN 200 to which server 1 belongs and the IP address of server 1. • Disable proxy ARP in VLAN 200.
ip route 1.1.1.10 255.255.255.255 1.1.1.1 ip route 2.2.2.10 255.255.255.255 2.2.2.1	These commands are used to configure a static route that diverts traffic destined for the server to the diversion interface on WAF.

WAF Configuration

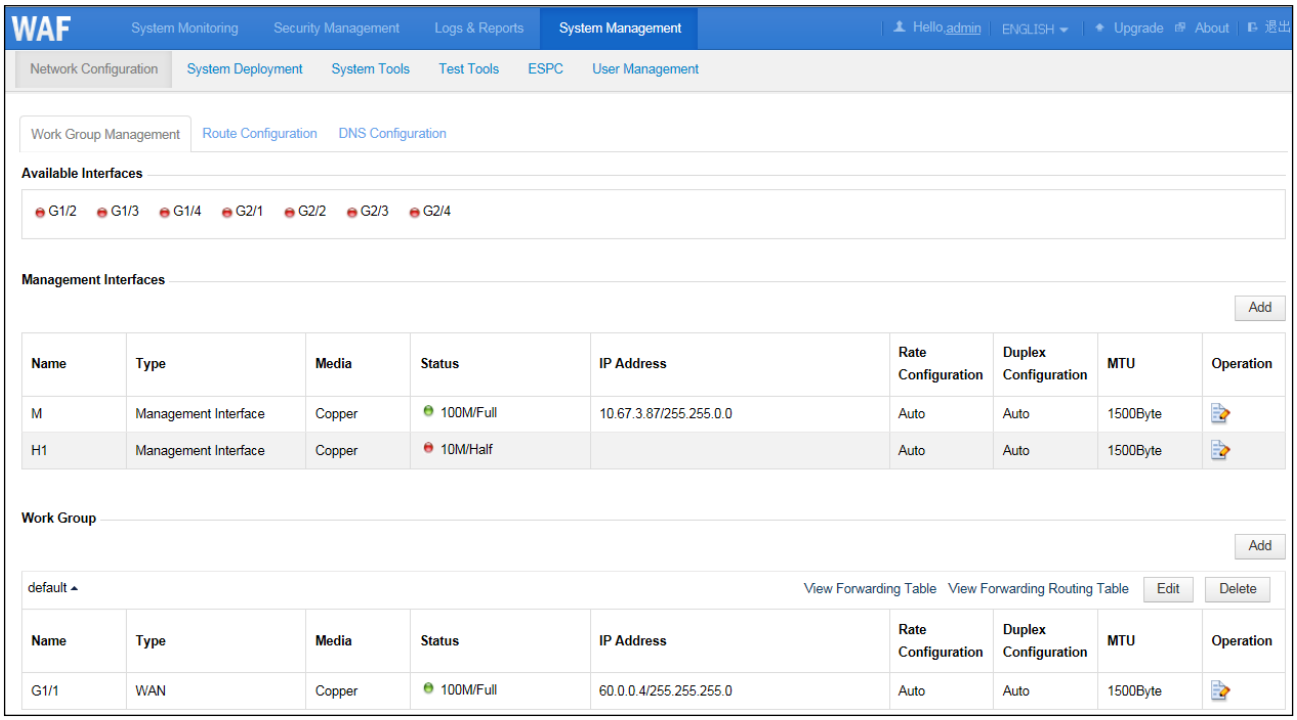
Note	• Both the diversion interface and the injection interface on WAF need to be configured as WAN interfaces that are in different network segments. • The injection interface needs to be configured with two subinterfaces.

Configuring the Diversion Interface and Injection Interface

Step 1 Create a work group.

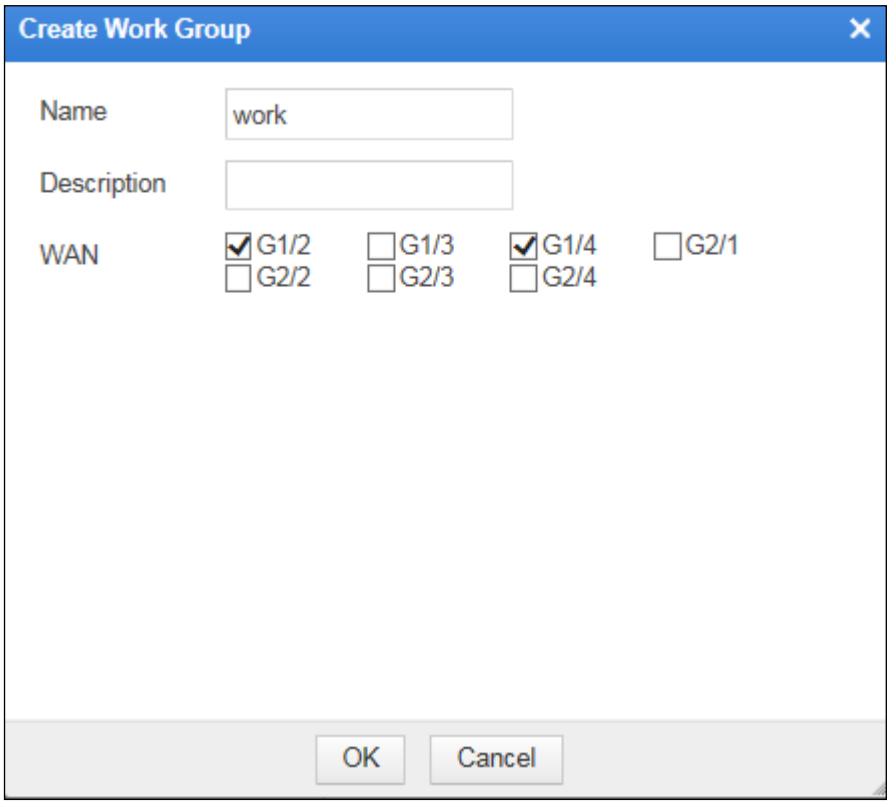
a. Choose **System Management** > **Network Configuration** > **Work Group Management**.

Figure 3-4 Layer 2 injection — Work Group Management page



b. In the lower-right corner of the work group list, click **Add** to add a work group (called **work** for example), using interfaces G1/2 and G1/4 as the injection interface and diversion interface respectively, as shown in Figure 3-5.

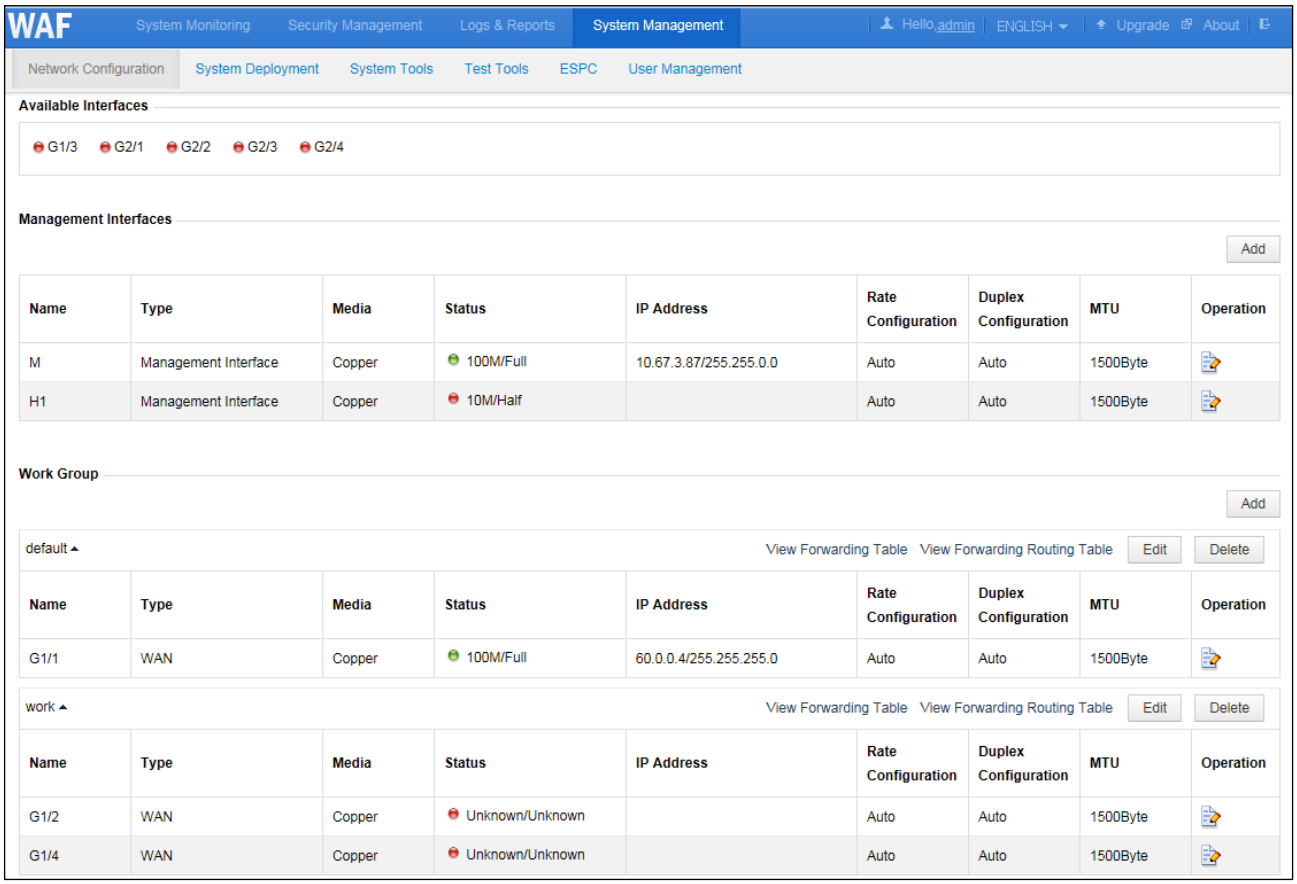
Figure 3-5 Layer 2 injection — creating a work group



c. Click **OK** to return to the **Work Group Management** page.

The new work group, **work**, appears on the page, as shown in Figure 3-6.

Figure 3-6 Layer 2 injection — new work group on the Work Group Management page

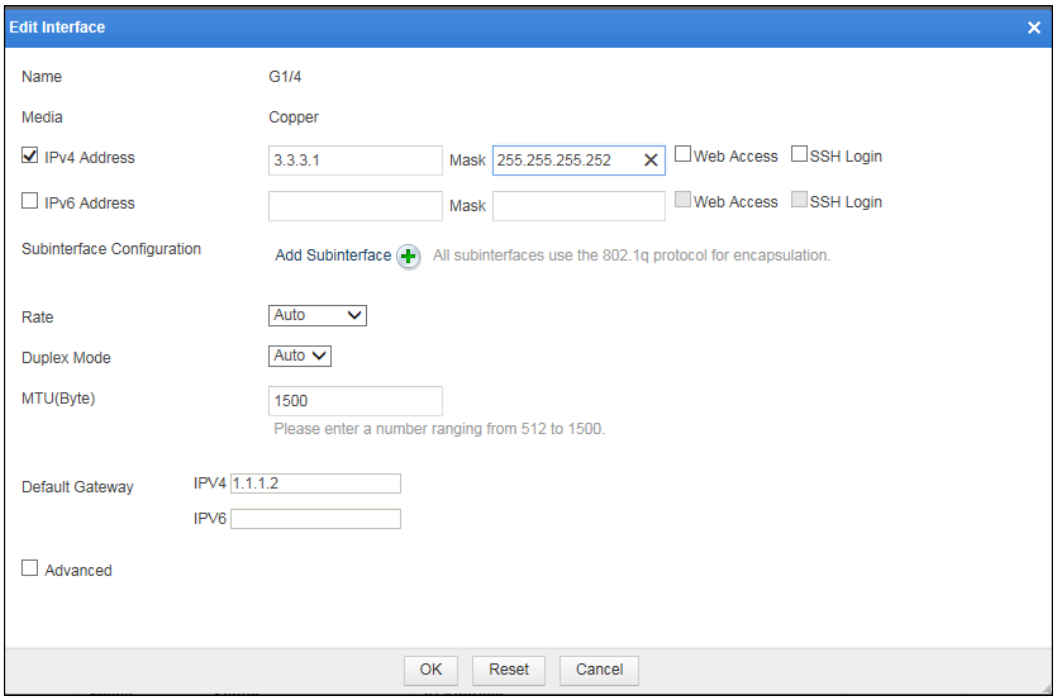


Step 2 Configure a diversion interface.

a. In the work group table shown in Figure 3-6, click in the row of interface G1/4 to configure interface parameters in the **Edit Interface** dialog box, as shown in Figure 3-7.

b. Click **OK** to complete the configuration.

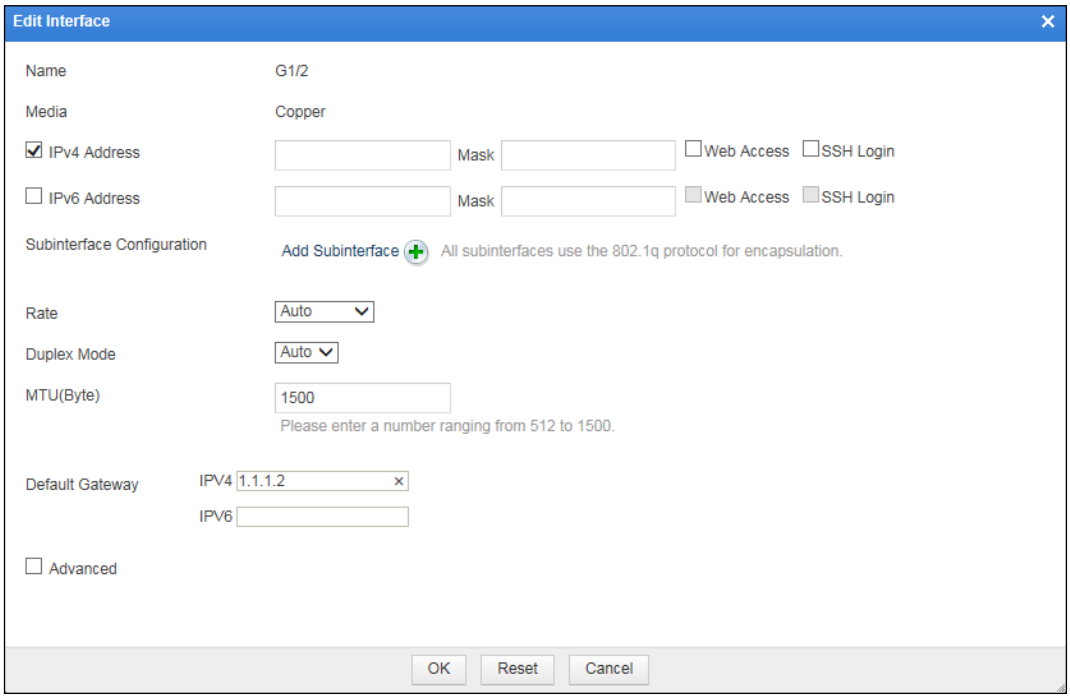
Figure 3-7 Layer 2 injection — editing diversion interface configuration



Step 3 Configure the injection interface.

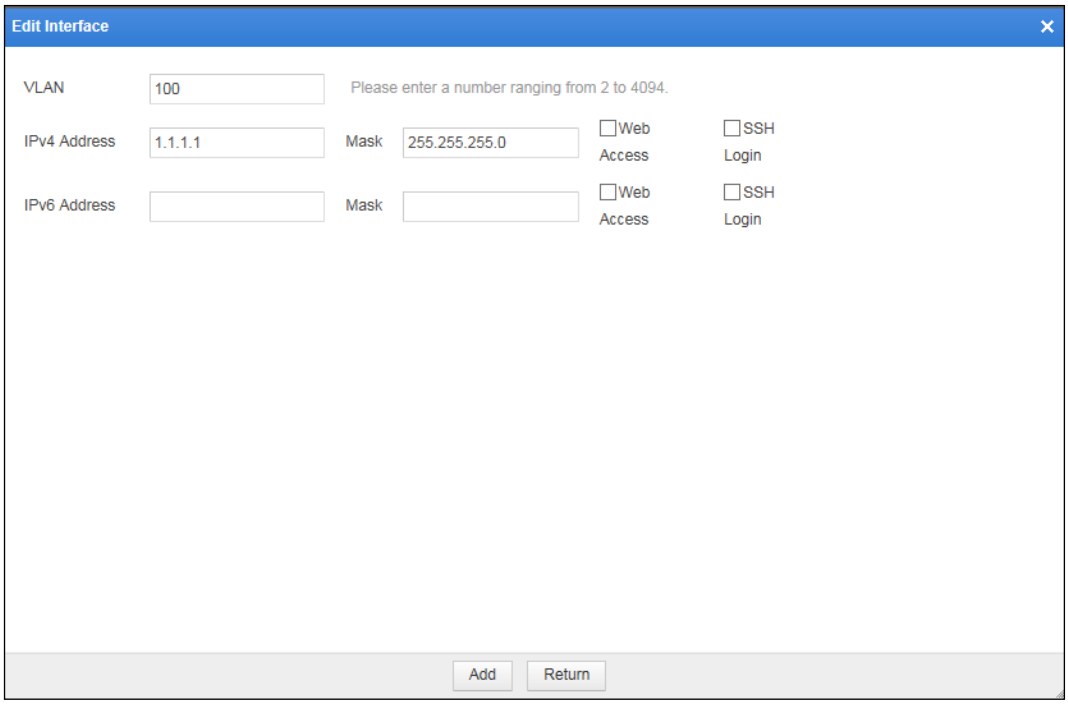
a. In the work group table shown in Figure 3-6, click in the row of interface G1/2 and configure interface parameters in the **Edit Interface** dialog box, as shown in Figure 3-8.

Figure 3-8 Layer 2 injection — editing injection interface configuration



b. In the **Edit Interface** dialog box shown in Figure 3-8, click the **Add Subinterface** link to add a subinterface for interface G1/2, for example VLAN 100, as shown in Figure 3-9.

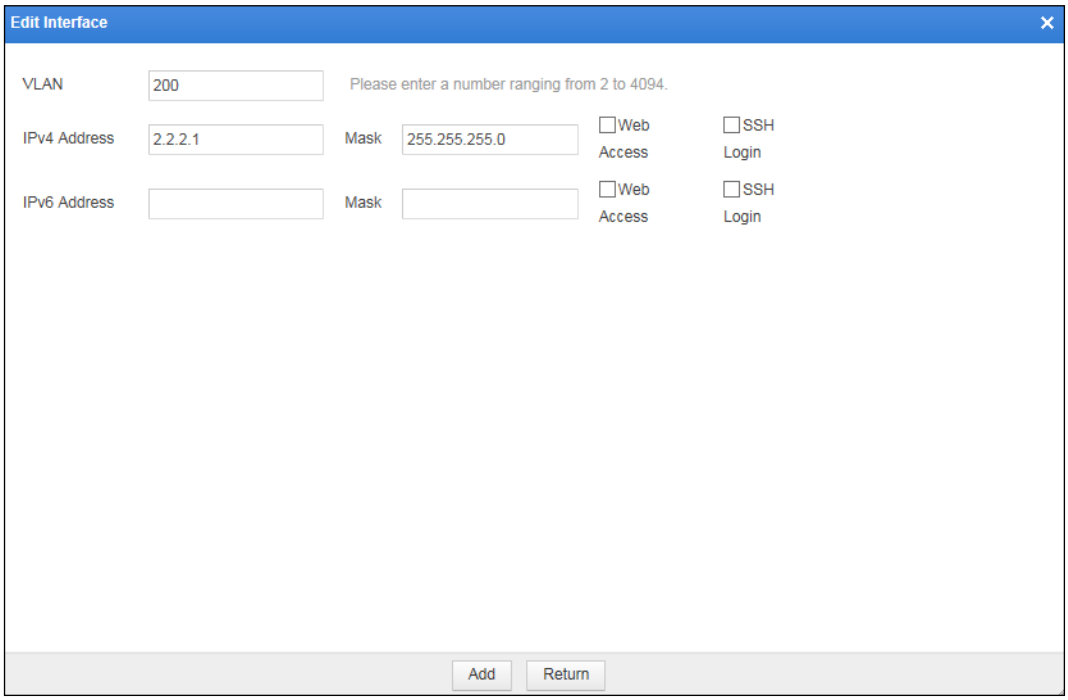
Figure 3-9 Layer 2 injection — adding subinterface 1



c. Click **Add** to successfully add VLAN 100 and return to the **Edit Interface** dialog box of interface G1/2.

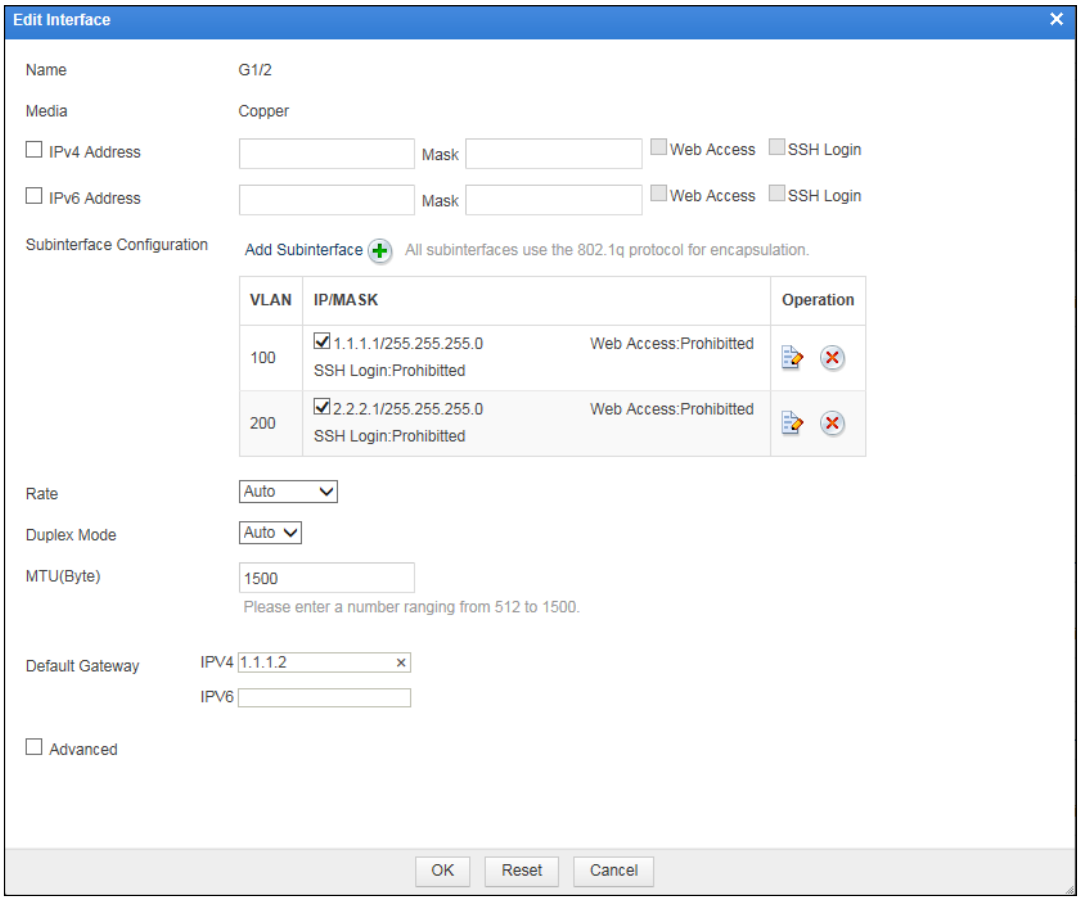
d. Re-click the **Add Subinterface** link to add the second subinterface, VLAN 200.

Figure 3-10 Layer 2 injection — adding subinterface 2



e. Click **Add** to successfully a dd VLAN 200 and return to the **Edit Interface** dialog box of interface G1/2.

Figure 3-11 Layer 2 injection — two subinterfaces of the injection interface



f. Click **OK** to complete the configuration.

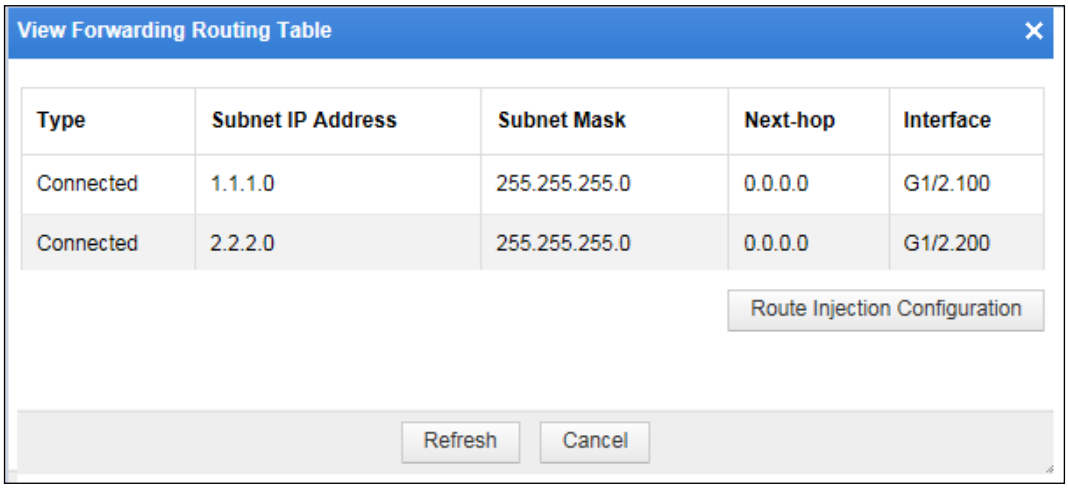
----End

Configuring an Injection Route

Note	After you configure IP addresses of injection subinterfaces, WAF has a direct route to the network segment of the server. You can check this route from the routing table, without configuring an injection route manually.

In the work group table shown in Figure 3-6, click the **View Forwarding Routing Table** link to view injection routes in the routing table, as shown in Figure 3-12.

Figure 3-12 Layer 2 injection — View Forwarding Routing Table dialog box

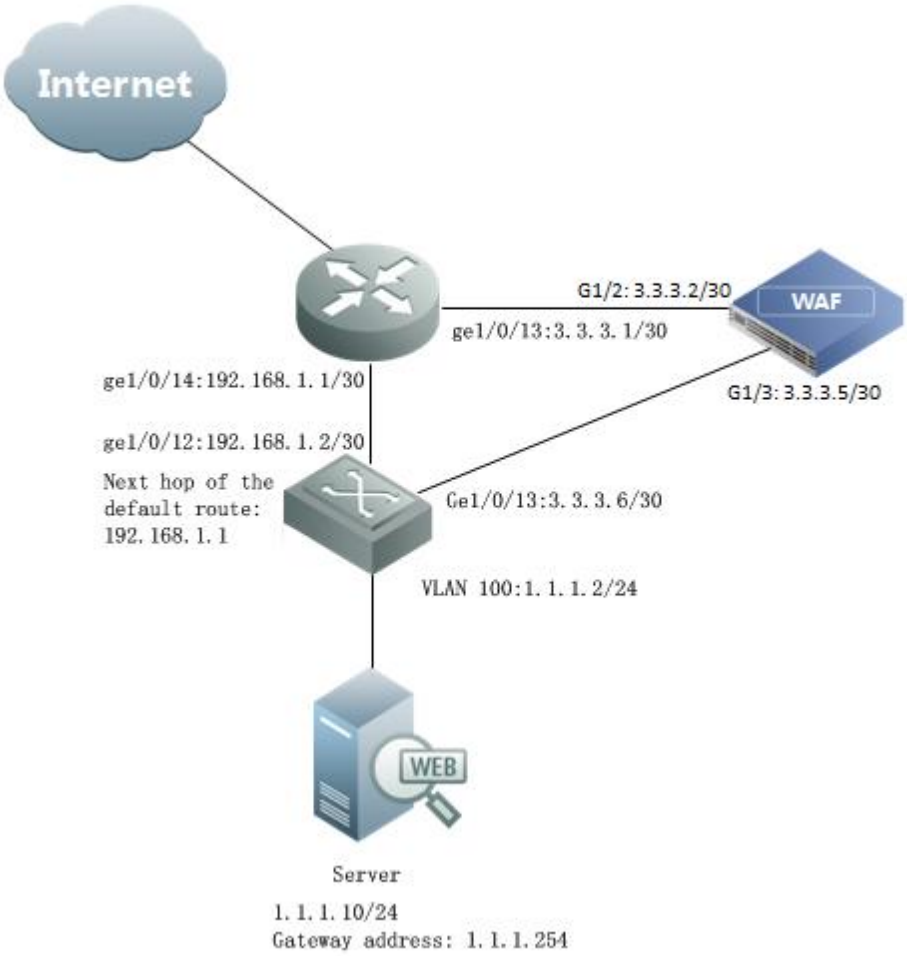


Type	Subnet IP Address	Subnet Mask	Next-hop	Interface
Connected	1.1.1.0	255.255.255.0	0.0.0.0	G1/2.100
Connected	2.2.2.0	255.255.255.0	0.0.0.0	G1/2.200

3.1.3 Crossover Injection

Figure 3-13 shows the crossover injection deployment topology.

Figure 3-13 Crossover injection — topology



Router and Switch Configuration

Router Configuration

Configuration Command	Description
interface GigabitEthernet1/0/11 description Connect-To-Internet no switchport ip address 10.10.10.1 255.255.255.0 !	These commands configure the interface used by the router to connect to the client (Internet).
interface GigabitEthernet1/0/13 description Connect-To- WAF-Diversion no switchport ip address 3.3.3.1 255.255.255.252 !	These commands configure the diversion interface as a layer 3 interface that directly connects to interface G1/2 on WAF.

Configuration Command	Description
interface GigabitEthernet1/0/14 no switchport ip address 192.168.1.1 255.255.255.0 !	These commands configure the IP address of the interface used by the router to connect to the downstream switch.
ip route 1.1.1.10 255.255.255.255 3.3.3.2 !	This command configures a static route from the server directly to the diversion interface on WAF.

Switch Configuration

Configuration Command	Description
interface GigabitEthernet1/0/12 no switchport ip address 192.168.1.2 255.255.255.252 !	These commands configure the IP address of the interface used by the switch to connect the router.
interface GigabitEthernet1/0/13 no switchport ip address 3.3.3.6 255.255.255.252 !	These commands configure the IP address of the injection interface connecting to WAF.
interface Vlan100 ip address 1.1.1.2 255.255.255.0 !	These commands configure VLAN 100.
interface GigabitEthernet1/0/21 switchport access vlan 100 switchport mode access !	These commands specify that the server's interface that connects to the switch belongs to VLAN 100.
ip route 0.0.0.0 0.0.0.0 192.168.1.1 !	This command configures a default route.

WAF Configuration

You need to configure the diversion interface, injection interface, and an injection route on WAF. The configuration method is the same as that in layer 2 injection mode. For details, see WAF Configuration in section 3.1.2 Layer 2 Injection.

3.1.4 PBR Injection

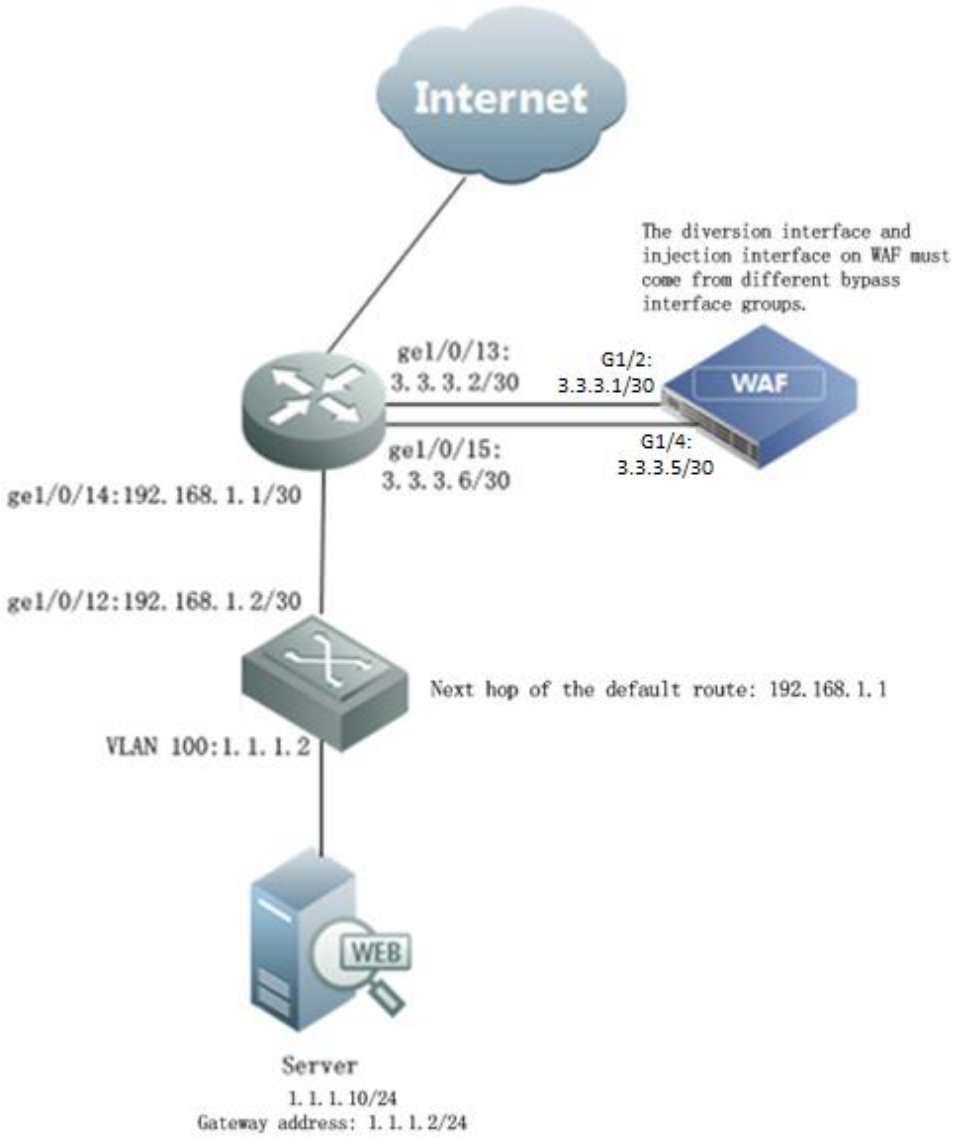
PBR injection include the following:

- Layer 3 Interface Injection
- Layer 3 Trunk Injection
- One-Arm Layer 3 Injection

3.1.4.1 Layer 3 Interface Injection

Figure 3-14 shows the layer 3 interface injection topology. On this topology, WAF uses interface G1/2 as the diversion interface and interface G1/4 as the injection interface.

Figure 3-14 Layer 3 interface injection — topology



Switch and Router Configuration

Router Configuration

Configuration Command	Description
interface GigabitEthernet1/0/11 description Connect-To-Internet no switchport ip address 10.10.10.1 255.255.255.0 !	These commands configure the interface used by the router to connect the client (Internet).
interface GigabitEthernet1/0/14 description Connect-To-Below-Router no switchport ip address 192.168.1.1 255.255.255.252 !	These commands configure the interface used by the router to connect to the downstream switch.
interface GigabitEthernet1/0/13 description Connect-To- WAF-Diversion no switchport ip address 3.3.3.2 255.255.255.252 !	These commands configure the diversion interface as a layer 3 interface that directly connects to interface G1/2 on WAF.
interface GigabitEthernet1/0/15 description Connect-To- WAF-Injection no switchport ip address 3.3.3.6 255.255.255.252 ip policy route-map waf !	These commands achieve the following: • Configure the injection interface that directly connects to interface G1/4 on WAF. • Apply the PBR (route-map named **WAF**) on the injection interface.
ip route 1.1.1.10 255.255.255.255 3.3.3.1 !	This command configures a static route from the server directly to the diversion interface of WAF.
access-list 100 permit ip any 1.1.1.0 0.0.0.255	This command configures an access control policy that only matches packets destined for 1.1.1.0/24, the network segment of the server.
route-map waf permit 10 match ip address 100 set ip next-hop 192.168.1.2 !	These commands configure a PBR. For packets destined for the network segment (access-list 100) of the server, the next-hop IP address is the IP address (192.168.1.2) of an interface on the router.

Switch Configuration

Configuration Command	Description
interface GigabitEthernet1/0/12 no switchport ip address 192.168.1.2 255.255.255.252 !	These commands configure the IP address of the interface used by the switch to connect to the upstream router.

Configuration Command	Description
interface Vlan100 ip address 1.1.1.2 255.255.255.0 !	These commands configure VLAN 100.
interface GigabitEthernet1/0/21 switchport access vlan 100 switchport mode access !	These commands specify that the server's interface that connects to the switch belongs to VLAN 100.
ip route 0.0.0.0 0.0.0.0 192.168.1.1 !	This command configures a default route.

WAF Configuration

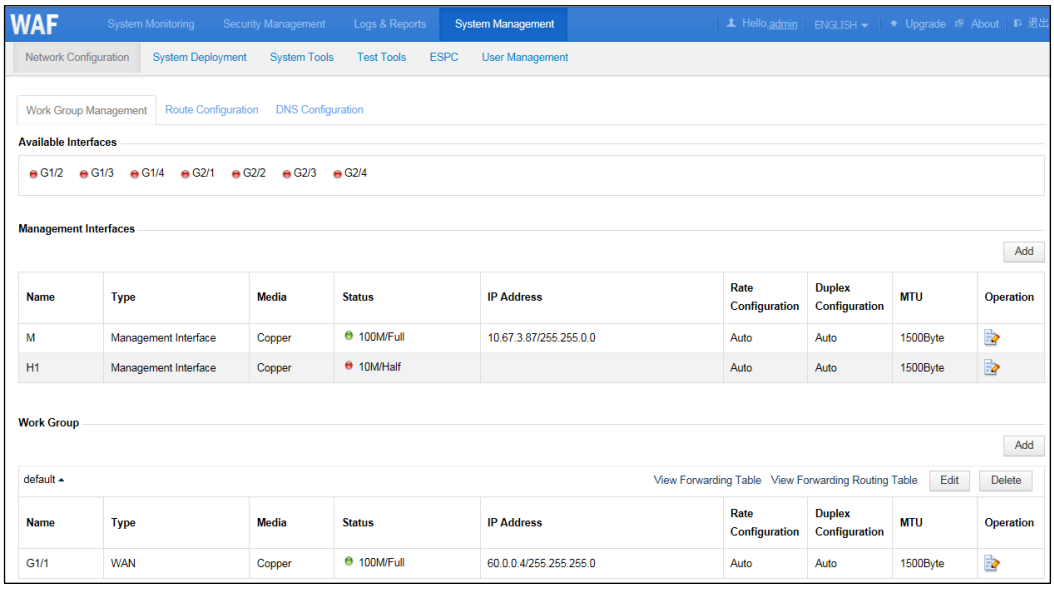
Note	• Both the diversion interface and injection interface on WAF need to be configured as WAN interfaces that are in different network segments. • No subinterface needs to be configured on the injection interface.

Configuring the Diversion Interface and Injection Interface

Step 1 Create a work group.

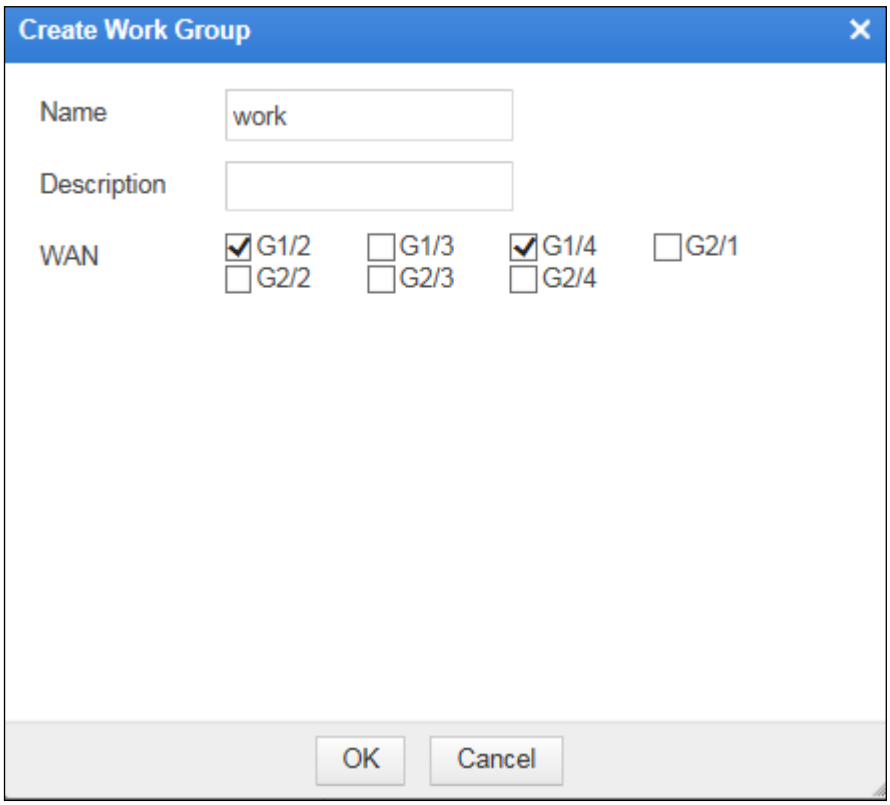
a. Choose **System Management** > **Network Configuration** > **Work Group Management**.

Figure 3-15 Layer 3 interface injection — Work Group Management page



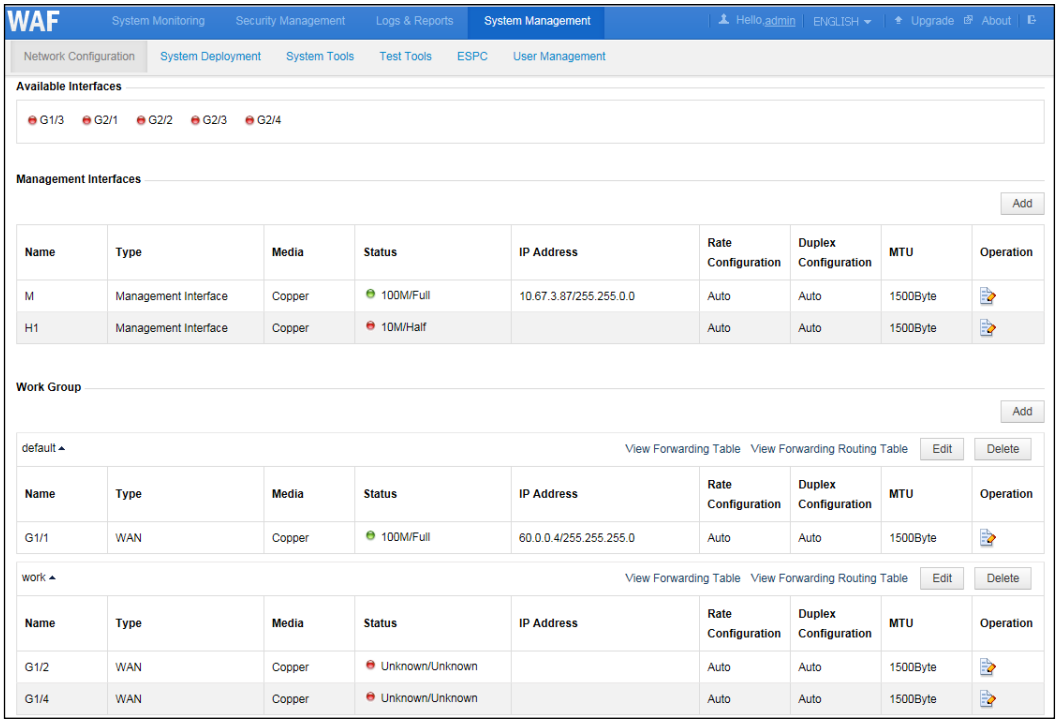
b. In the lower-right corner of the work group list shown in Figure 3-15, click **Add** to add a work group, using interface G1/2 and G1/4 as the diversion interface and injection interface respectively, as shown in Figure 3-16.

Figure 3-16 Layer 3 interface injection — Create Work Group dialog box



c. Click **OK** to return to the **Work Group Management** page, as shown in Figure 3-17.

Figure 3-17 Layer 3 interface injection — new work group on the Work Group Management page

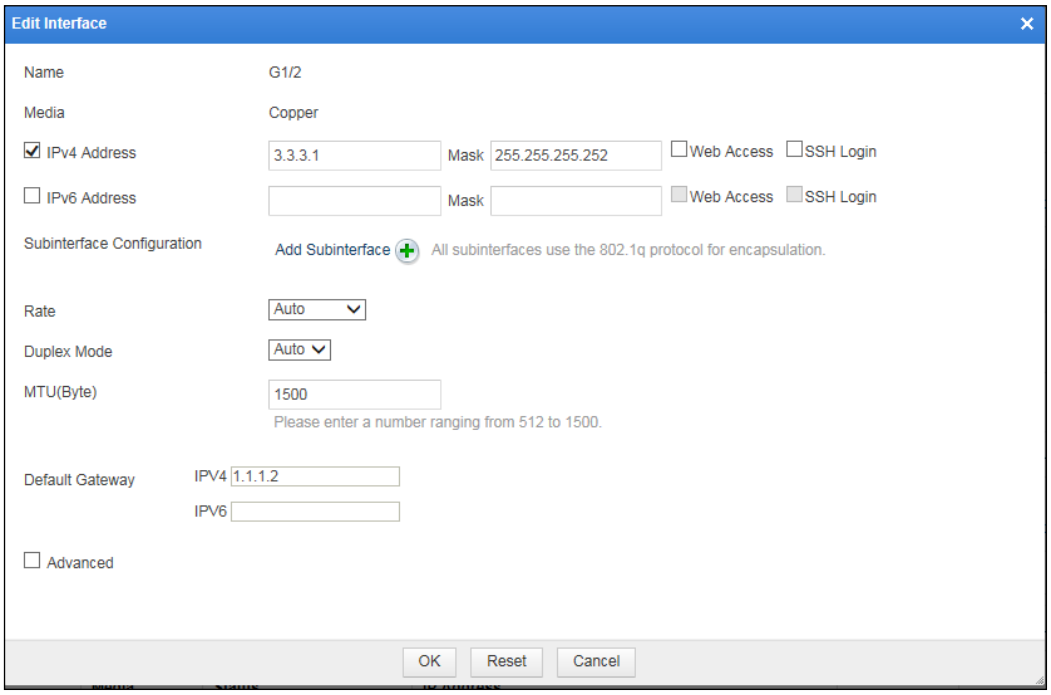


Step 2 Configure the diversion interface.

a. Click in the row of interface G1/2 and configure interface parameters in the **Edit Interface** dialog box, as shown in Figure 3-18.

b. Click **OK** to complete the configuration.

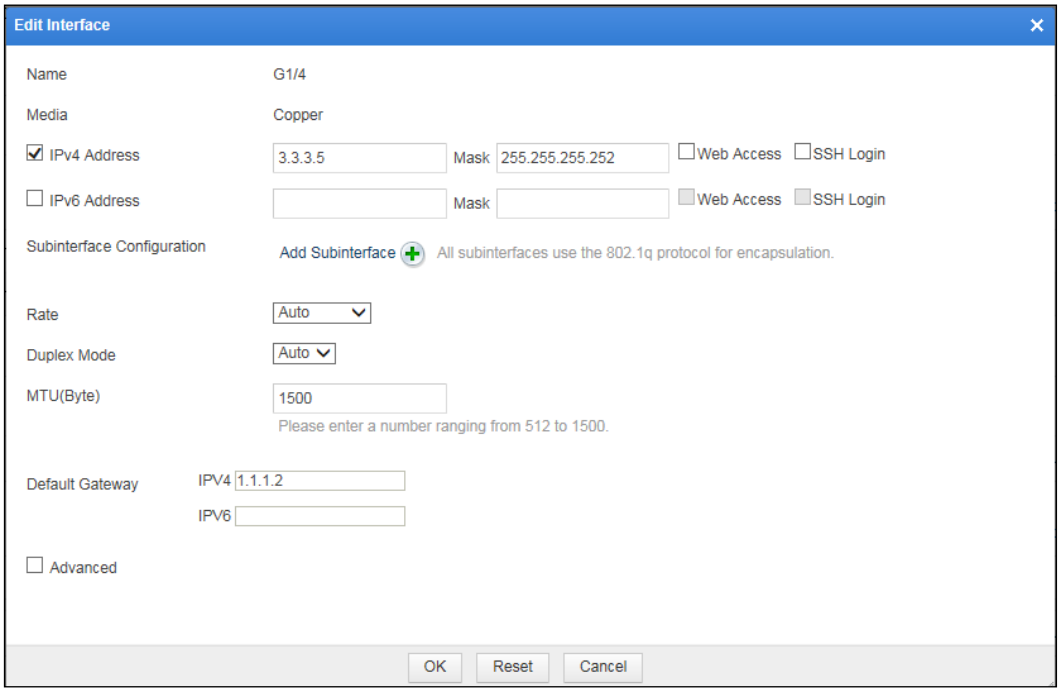
Figure 3-18 Layer 3 interface injection — editing diversion interface configuration



Step 3 Configure the injection interface.

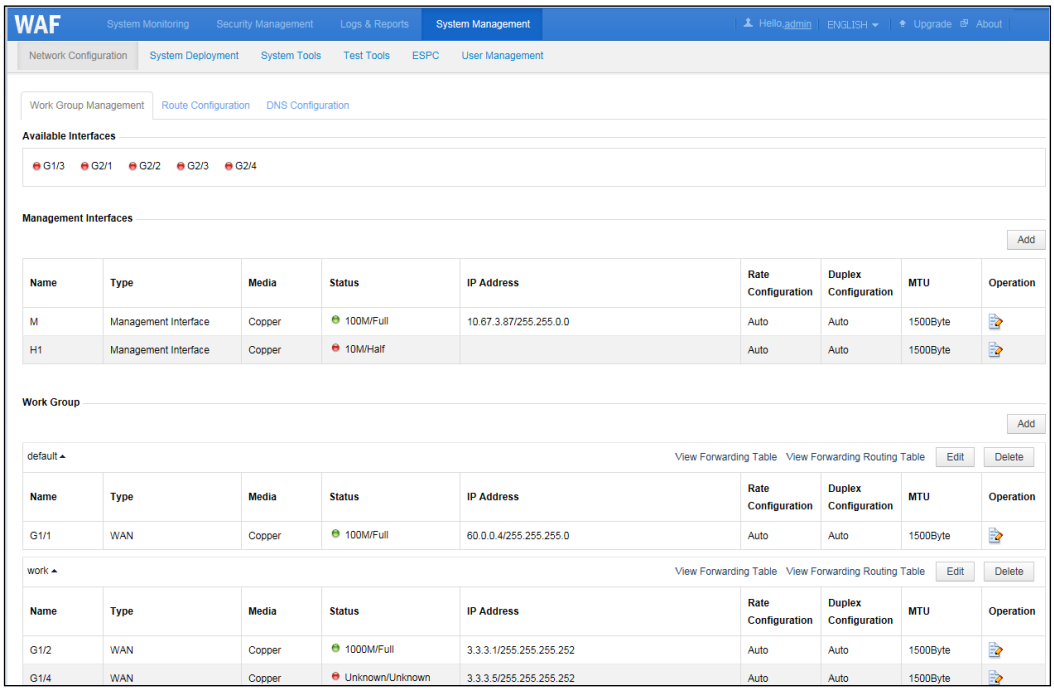
a. Click in the row of interface G1/4 and configure interface parameters in the **Edit Interface** dialog box, as shown in Figure 3-19.

Figure 3-19 Layer 3 interface injection — editing injection interface configuration



b. Click **OK** to complete the configuration and return to the **Work Group Management** page, as shown in Figure 3-20.

Figure 3-20 Layer 3 interface injection — interface configuration on the Work Group Management page



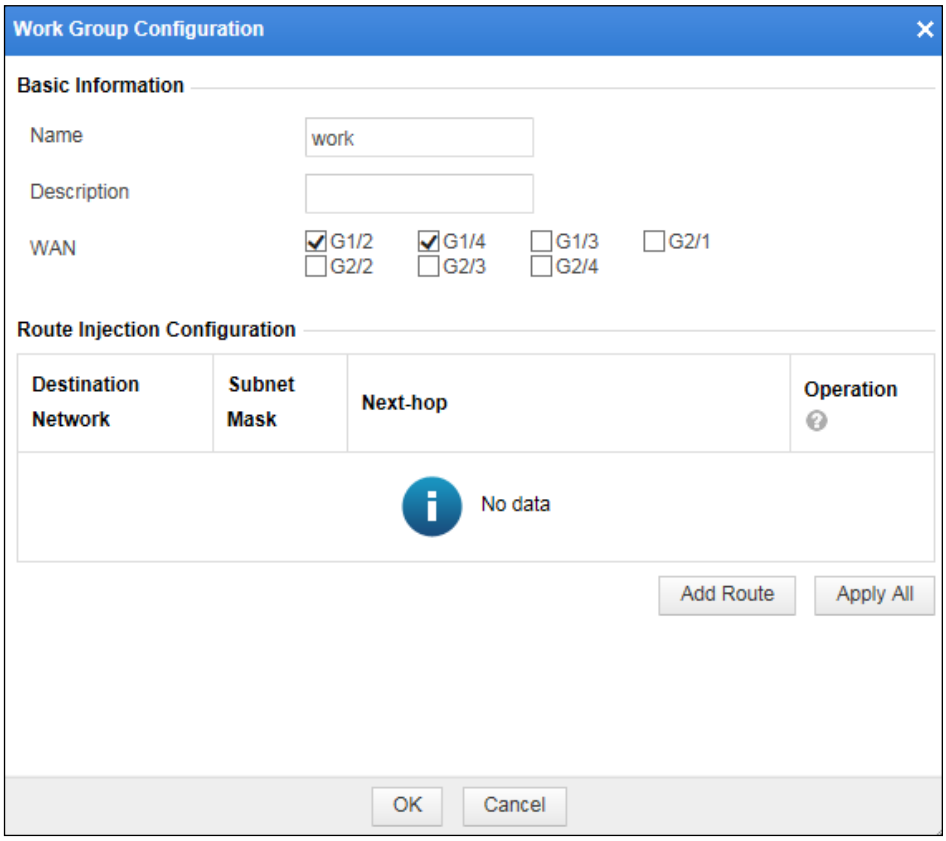
----End

Configuring an Injection Route

Step 1 On the **Work Group Management** page shown in Figure 3-20, click **Edit** in the upper-right corner of the **work** group.

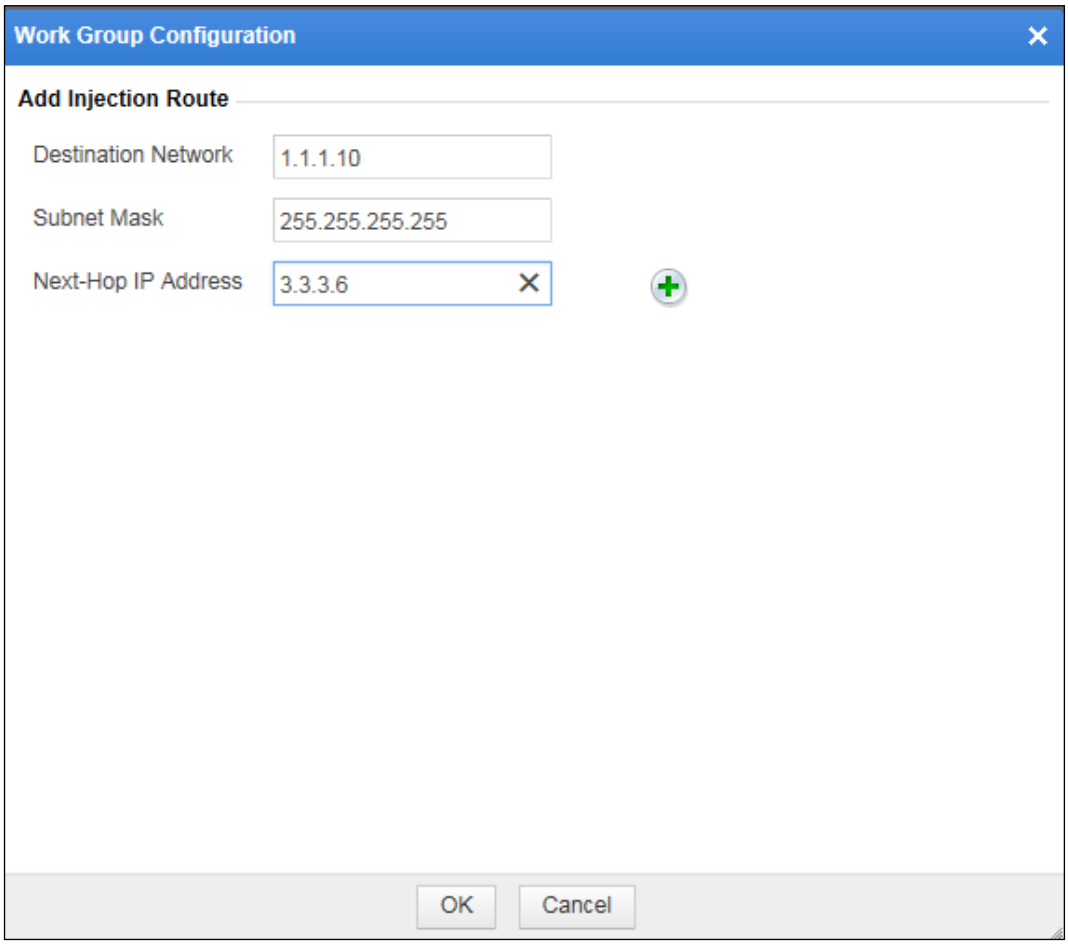
The **Work Group Configuration** dialog box appears, as shown in Figure 3-21.

Figure 3-21 Layer 3 interface injection — editing a work group



Step 2 In the lower-right corner of the injection route list, click **Add Route** to add an injection route, as shown in Figure 3-22.

Figure 3-22 Layer 3 Interface injection — adding an injection route



Note	**Destination Network** (1.1.1.10) is the IP address of the server, and **Next-Hop IP Address** (3.3.3.6) is the IP address of the injection interface on the switch directly connected to WAF.

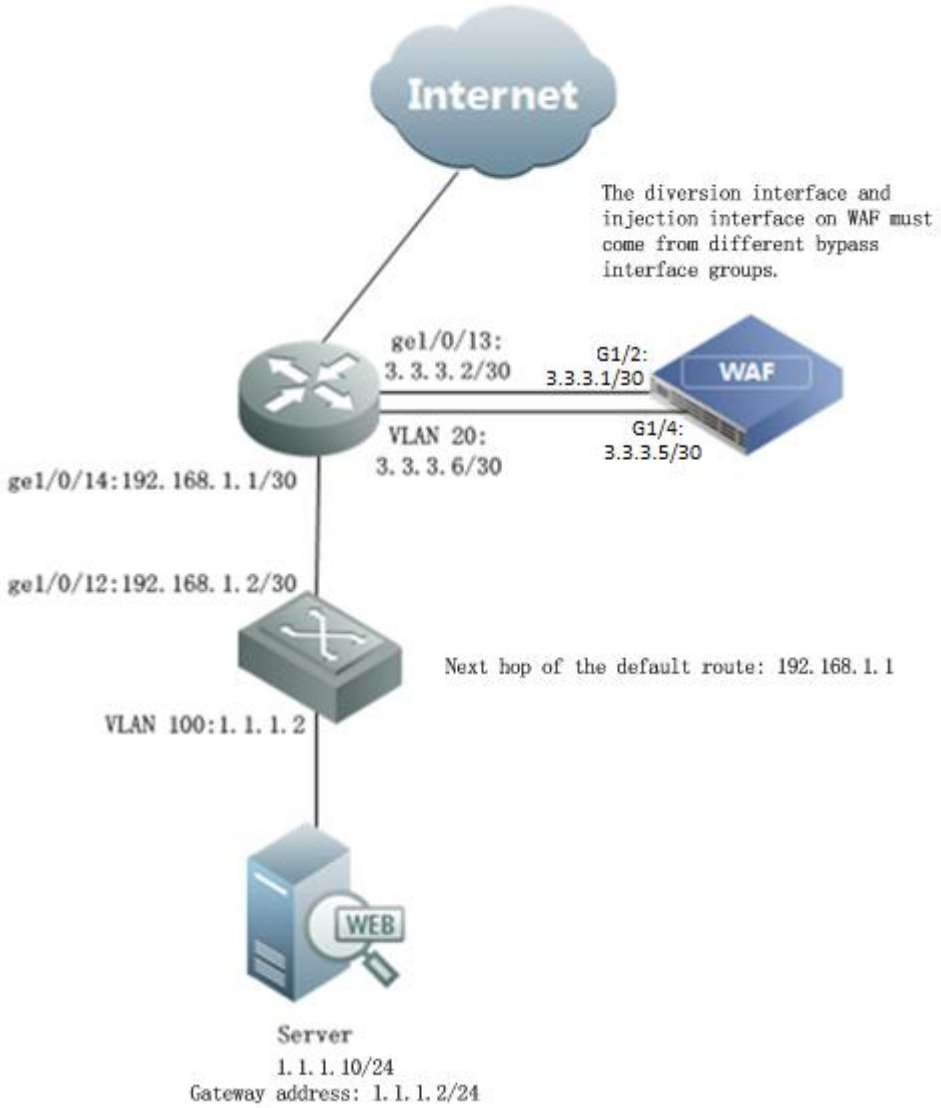
Step 3 Click **OK** to complete the configuration.

----End

3.1.4.2 Layer 3 Trunk Injection

As shown in Figure 3-23, the router directly connects to WAF and the Internet, and the switch connects to the server. The router directly connecting to WAF uses a layer 3 interface as the diversion interface and uses a trunk interface as the injection interface. WAF uses interface G1/2 as the diversion interface and interface G1/4 as the injection interface.

Figure 3-23 Layer 3 trunk injection — topology



Router and Switch Configuration

Router Configuration

Configuration Command	Description
interface GigabitEthernet1/0/11 description Connect-To-Internet no switchport ip address 10.10.10.1 255.255.255.0 !	These commands configure the interface used by the router to connect to the client (Internet).

Configuration Command	Description
interface GigabitEthernet1/0/14 description Connect-To-Below-Router no switchport ip address 192.168.1.1 255.255.255.252 !	These commands configure the interface used by the router to connect to the downstream switch.
interface GigabitEthernet1/0/13 description Connect-To- WAF-Diversion no switchport ip address 3.3.3.2 255.255.255.252 !	These commands configure the diversion interface as a layer 3 interface that directly connects to interface G1/2 on WAF
interface GigabitEthernet1/0/15 description Connect-To-Inject-WAF switchport trunk encapsulation dot1q switchport trunk allowed vlan 20 switchport mode trunk !	These commands configure an injection interface that: • Directly connects to interface G1/4 on WAF. • Works in trunk mode and uses dot1q encapsulation. • Allows traffic from VLAN 20 to pass through.
ip route 1.1.1.10 255.255.255.255 3.3.3.1 !	This command configures a static route from the server directly to the diversion interface of WAF.
access-list 100 permit ip any 1.1.1.0 0.0.0.255 !	This command configures an access control policy that only matches packets destined for 1.1.1.0/24, the network segment of the server.
route-map waf permit 10 match ip address 100 set ip next-hop 192.168.1.2 !	These commands configure a PBR. For packets destined for the network segment (access-list 100) of the server, the next-hop IP address is the IP address (192.168.1.2) of an interface on the router.
interface Vlan20 description Injection ip address 3.3.3.6 255.255.255.252 ip policy route-map waf !	These commands configure VLAN 20 and apply the PBR (route-map named **waf**) on it.

Switch Configuration

Configuration Command	Description
interface GigabitEthernet1/0/12 no switchport ip address 192.168.1.2 255.255.255.252 !	These commands configure the IP address of the interface used by the switch to connect to the router.
interface Vlan100 ip address 1.1.1.2 255.255.255.0 no ip proxy-arp !	This command configures VLAN 100.
interface GigabitEthernet1/0/21 switchport access vlan 100 switchport mode access !	These commands specify that the server's interface that connects to the switch belongs to VLAN 100.
ip route 0.0.0.0 0.0.0.0 192.168.1.1 !	This command configures a default route.

WAF Configuration

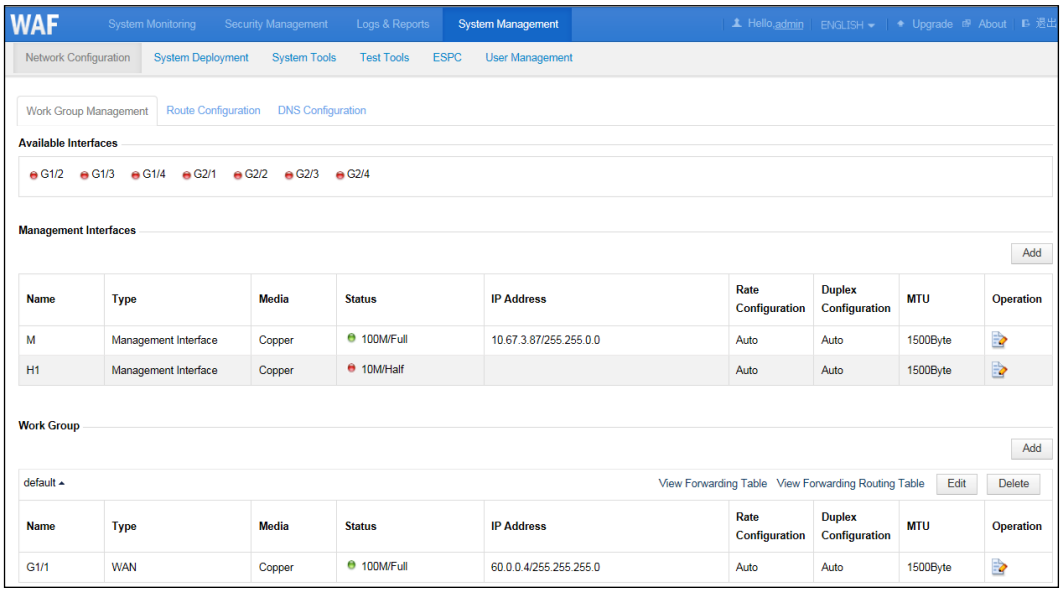
Note	• Both the diversion interface and injection interface on WAF need to be configured as WAN interfaces that are in different network segments. • The injection interface (G1/4) is deployed in trunk mode and needs subinterfaces only.

Configuring the Diversion Interface and Injection Interface

Step 1 Create a work group.

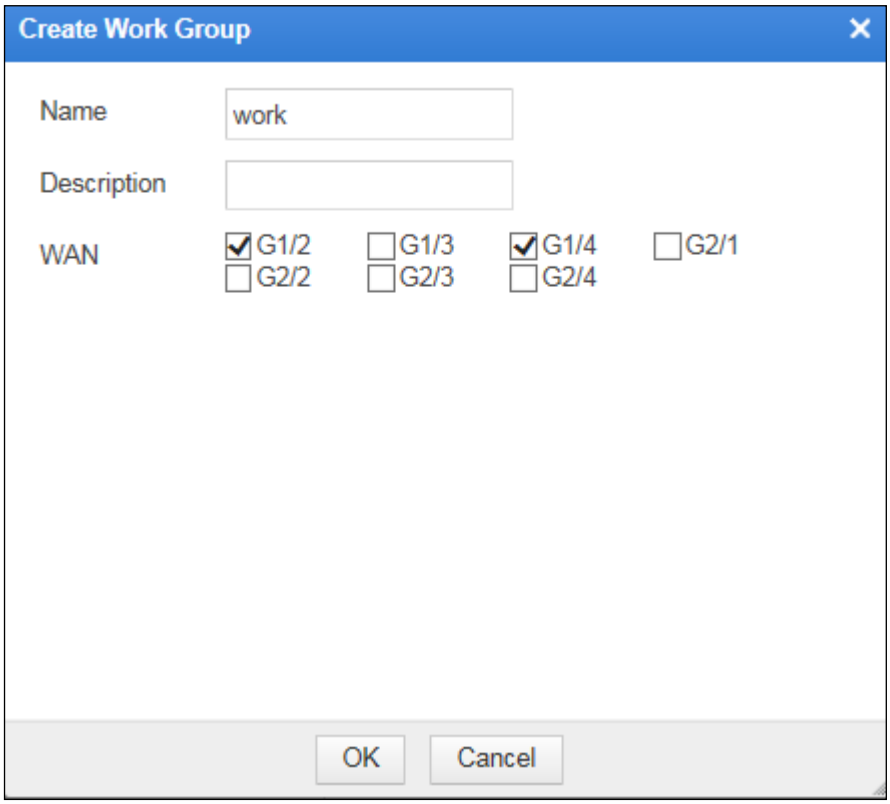
a. Choose **System Management** > **Network Configuration** > **Work Group Management**.

Figure 3-24 Layer 3 trunk injection — Work Group Management page



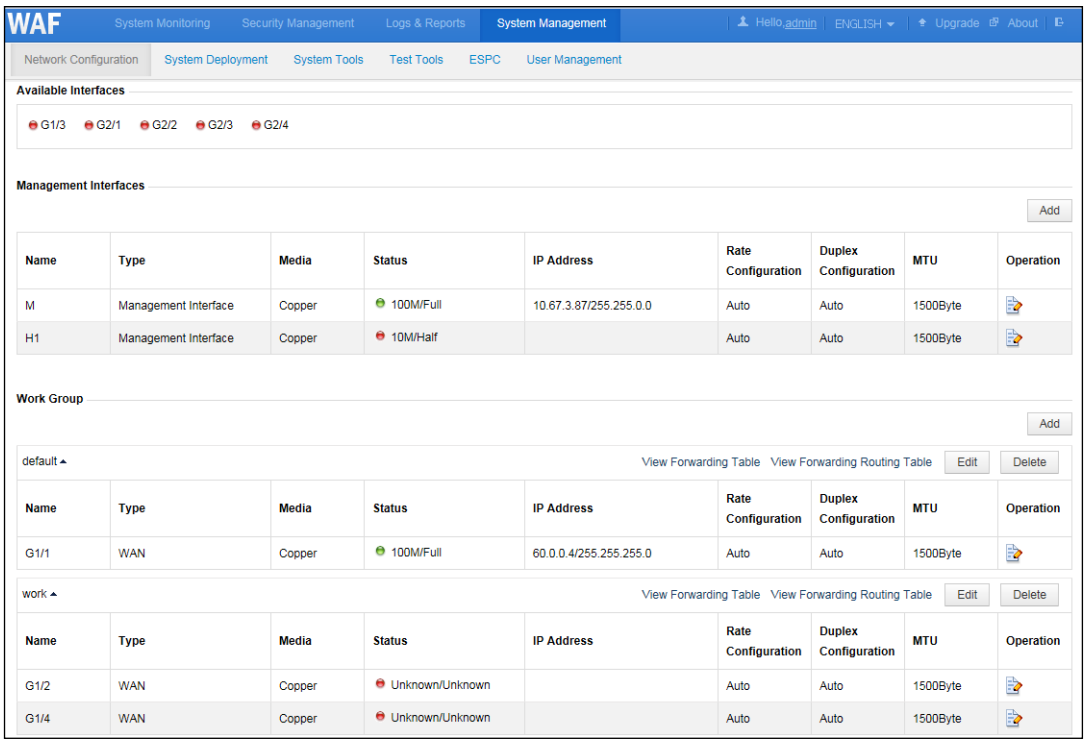
b. In the lower-right corner of the work group list, click **Add** to add a work group, using interfaces G1/2 and G1/4 as the diversion interface and injection interface respectively, as shown in Figure 3-25.

Figure 3-25 Layer 3 trunk injection — Create Work Group dialog box



c. Click **OK** to return to the **Work Group Management** page, as shown in Figure 3-26.

Figure 3-26 Layer 3 trunk injection — new work group on the Work Group Management page

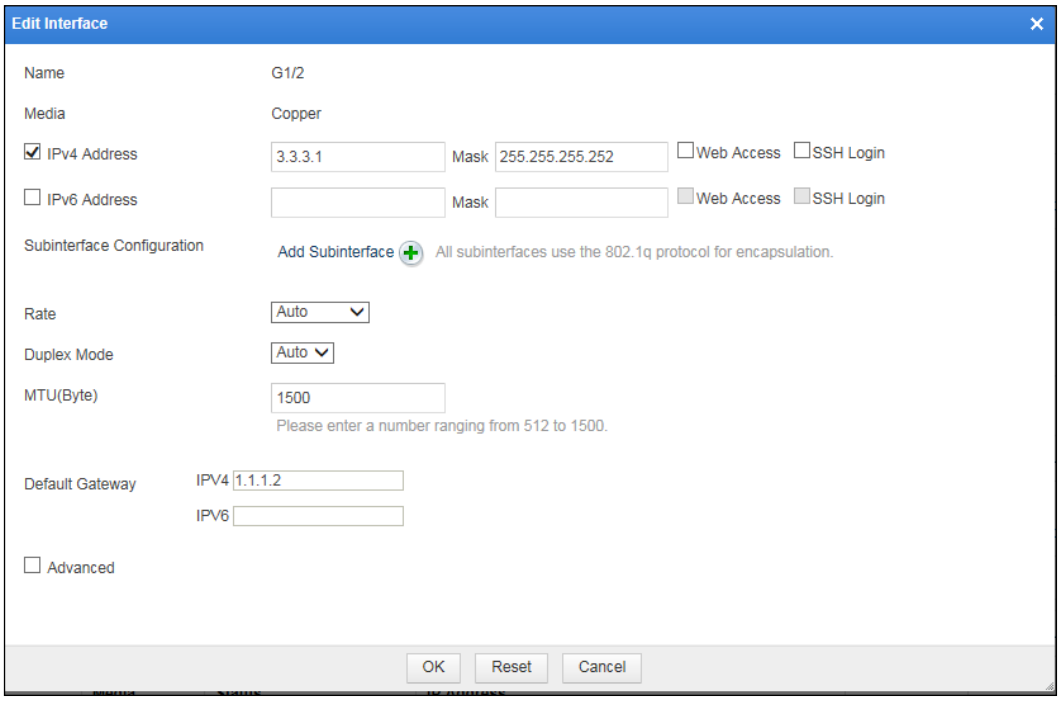


Step 2 Configure the diversion interface.

a. Click in the row of interface G1/2 to edit interface parameters in the **Edit Interface** dialog box, as shown in Figure 3-27.

b. Click **OK** to complete the configuration.

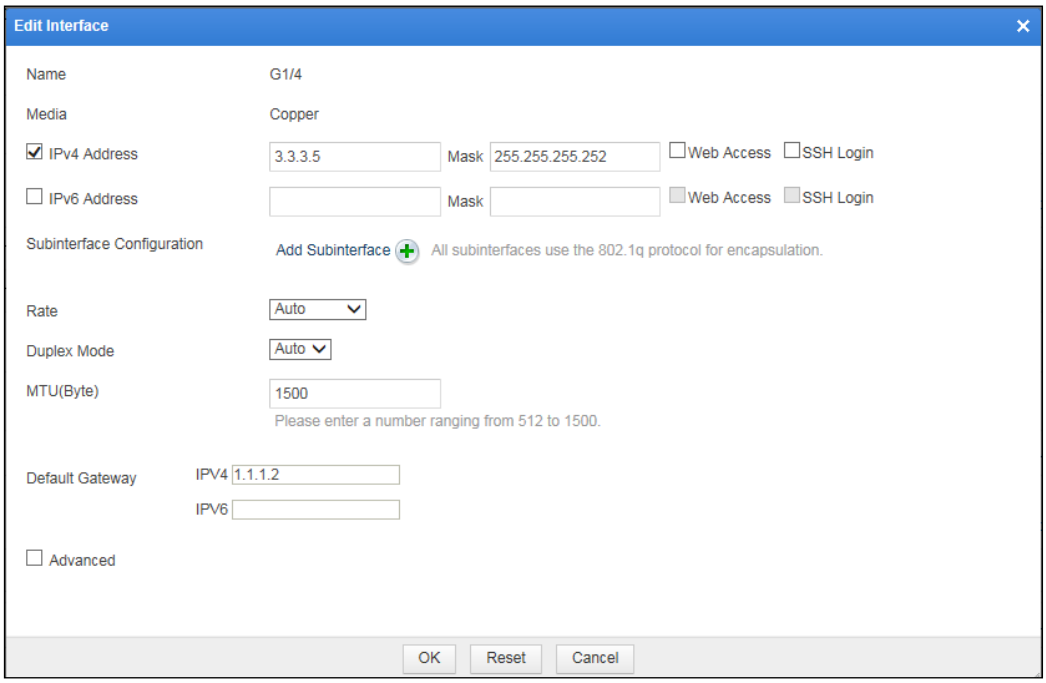
Figure 3-27 Layer 3 trunk injection — editing the diversion interface



Step 3 Configure the injection interface.

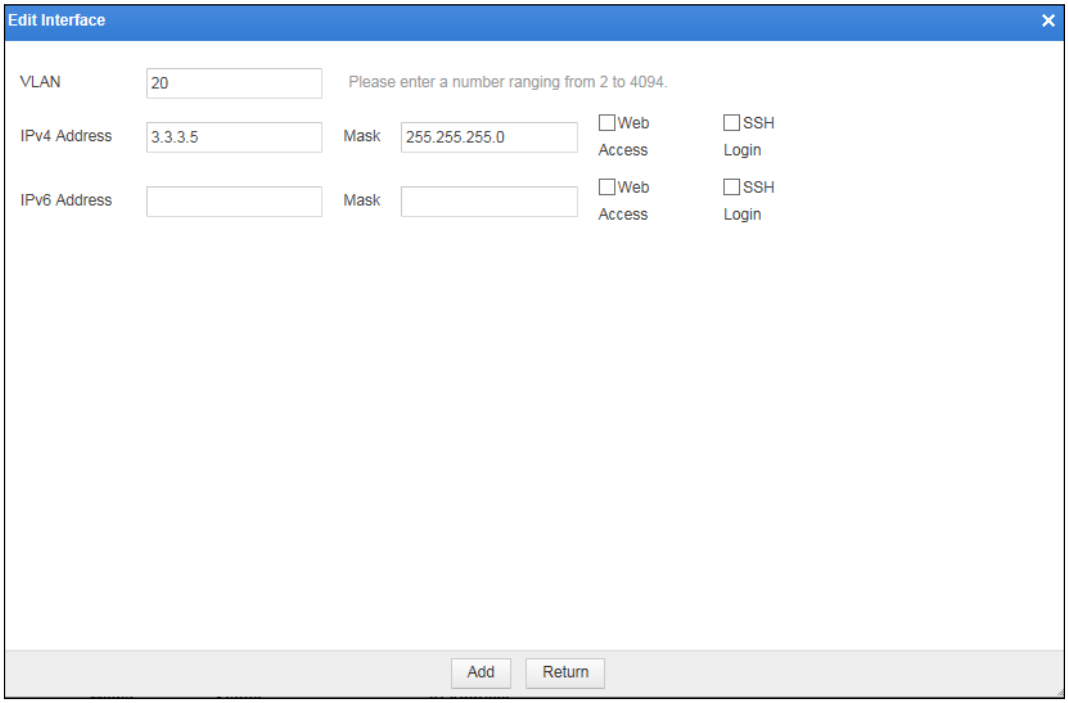
a. In the work group table shown in Figure 3-26, click in the row of interface G1/4 to edit interface parameters in the **Edit Interface** dialog box, as shown in Figure 3-28.

Figure 3-28 Layer 3 trunk injection — editing the injection interface



b. Click the **Add Subinterface** link to add a subinterface, for example, VLAN 20, as shown in Figure 3-29.

Figure 3-29 Layer 3 trunk injection — adding a subinterface



c. Click **Add** to complete the configuration.

----End

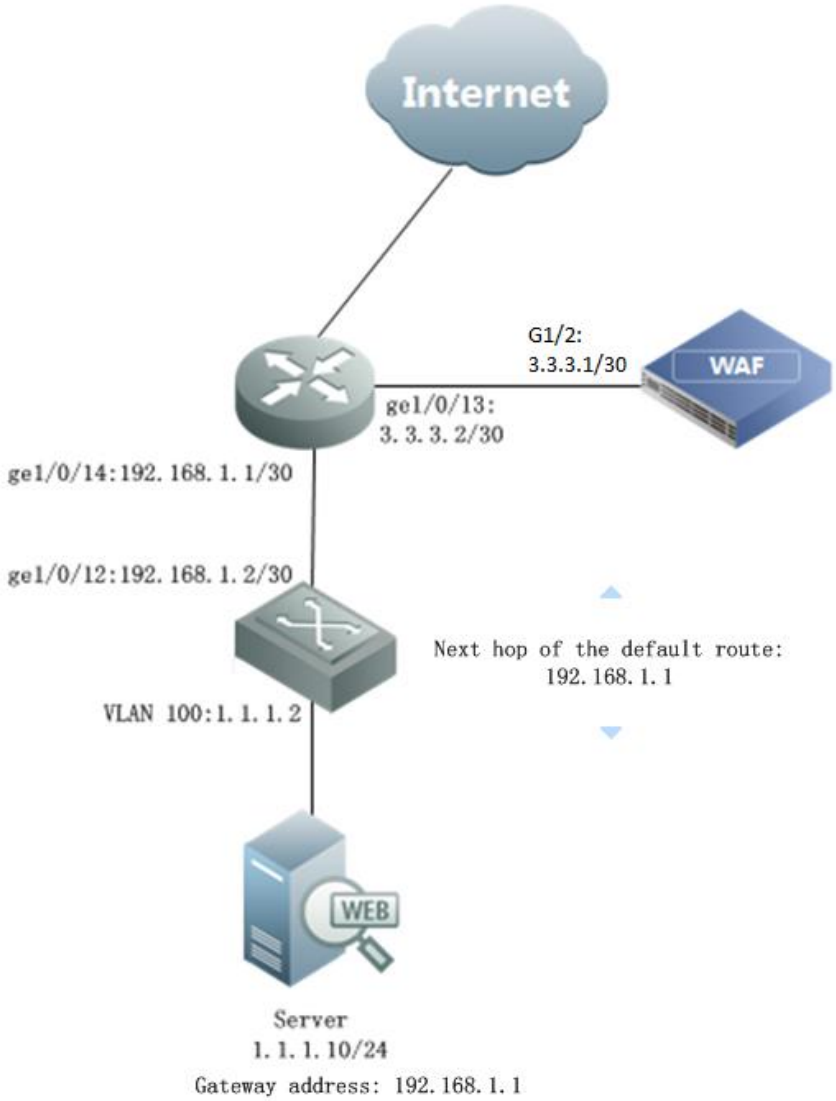
Configuring an Injection Route

In this mode, the injection route is configured in the same way as the layer 3 interface injection mode. For details, see Configuring an Injection Route in section 3.1.4.1 Layer 3 Interface Injection.

3.1.4.3 One-Arm Layer 3 Injection

Figure 3-30 shows the one-arm layer 3 injection topology. In this mode, both the diversion interface and injection on WAF are interface G1/2.

Figure 3-30 One-Arm layer 3 injection — topology



Router and Switch Configuration

Router Configuration

Configuration Command	Description
interface GigabitEthernet1/0/11 description Connect-To-Internet no switchport ip address 10.10.10.1 255.255.255.0 !	These commands configure the interface used by the router to connect the client (Internet).

Configuration Command	Description
interface GigabitEthernet1/0/14 description Connect-To-Below-Router no switchport ip address 192.168.1.1 255.255.255.252 !	These commands configure the interface used by the router to connect to the downstream switch.
interface GigabitEthernet1/0/13 description Connect-To- WAF-Diversion no switchport ip address 3.3.3.2 255.255.255.252 ip policy route-map waf !	These commands achieve the following: • Configure a diversion interface as a layer 3 interface that connects to interface G1/2 on WAF. • Apply the PBR (route-map named **WAF**) on the diversion interface.
ip route 1.1.1.10 255.255.255.255 3.3.3.1 !	This command configures a static route that diverts traffic destined for the server to the diversion interface on WAF.
access-list 100 permit ip any 1.1.1.0 0.0.0.255 !	This command configures an access control policy that only matches packets destined for 1.1.1.0/24, the network segment of the server.
route-map waf permit 10 match ip address 100 set ip next-hop 192.168.1.2 !	These commands configure a PBR. For packets destined for the network segment (access-list 100) of the server, the next-hop IP address is the IP address (192.168.1.2) of an interface on the router.

Switch Configuration

Configuration Command	Description
interface GigabitEthernet1/0/12 no switchport ip address 192.168.1.2 255.255.255.252 !	These commands configure the IP address of the interface used by the switch to connect to the router.
interface Vlan100 ip address 1.1.1.2 255.255.255.0 !	This command configures VLAN 100.
interface GigabitEthernet1/0/21 switchport access vlan 100 switchport mode access !	These commands specify that the server's interface that connects to the switch belongs to VLAN 100.

Configuration Command	Description
ip route 0.0.0.0 0.0.0.0 192.168.1.1 !	This command configures a default route.

WAF Configuration

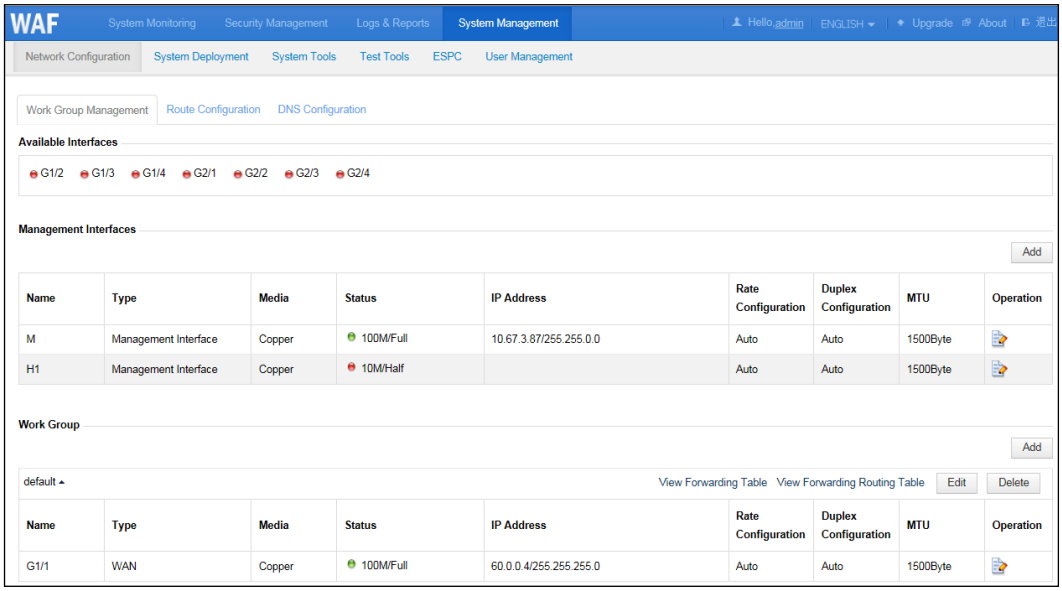
Note	Interface G1/2 (a WAN interface) is configured as both the diversion interface and injection interface.

Configuring the Interface

Step 1 Create a work group.

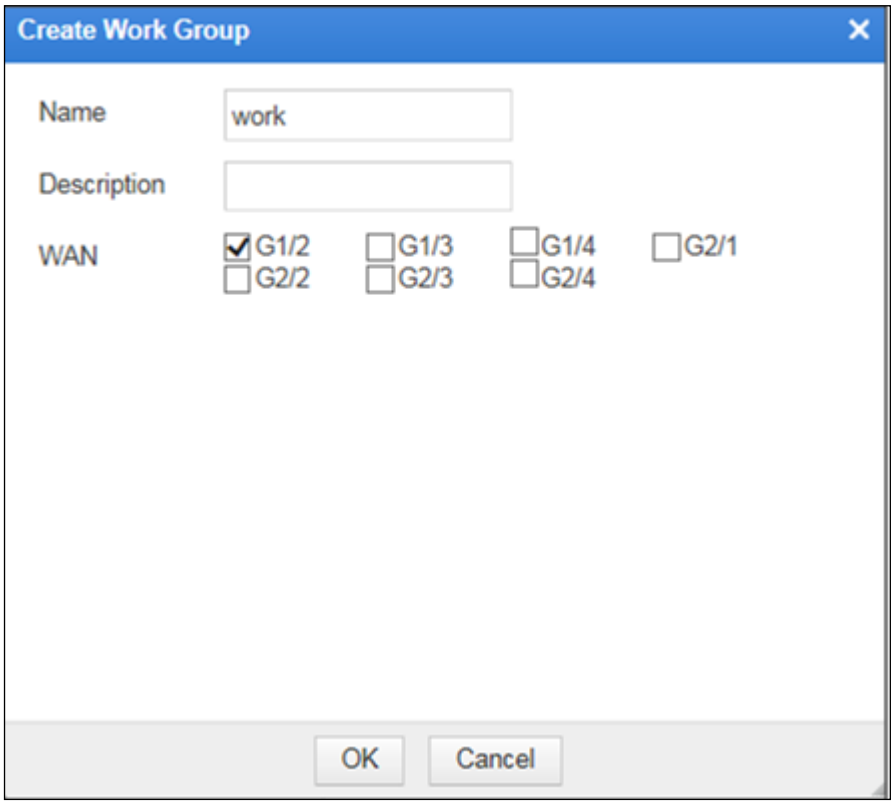
a. Choose **System Management** > **Network Configuration** > **Work Group Management**.

Figure 3-31 One-arm layer 3 injection — Work Group Management page



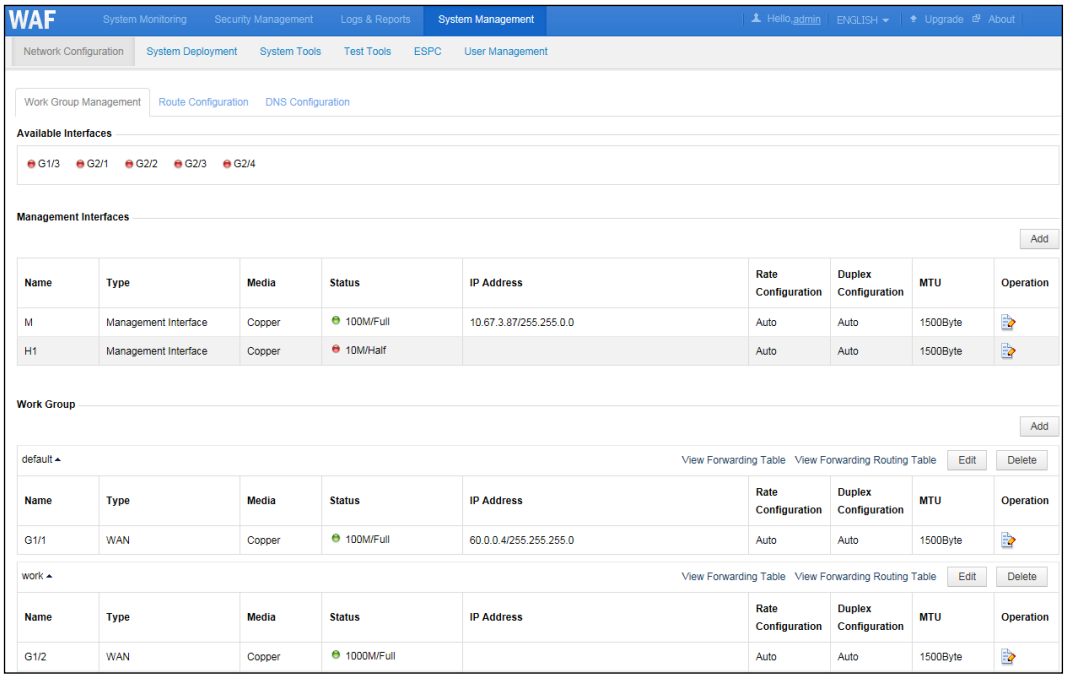
b. In the lower-right corner of the work group list, click **Add** to add a work group, using interface G1/2 as both the diversion interface and injection interface, as shown in Figure 3-32.

Figure 3-32 One-arm layer 3 injection — Create Work Group dialog box



c. Click **OK** to return to the **Work Group Management** page, as shown in Figure 3-33.

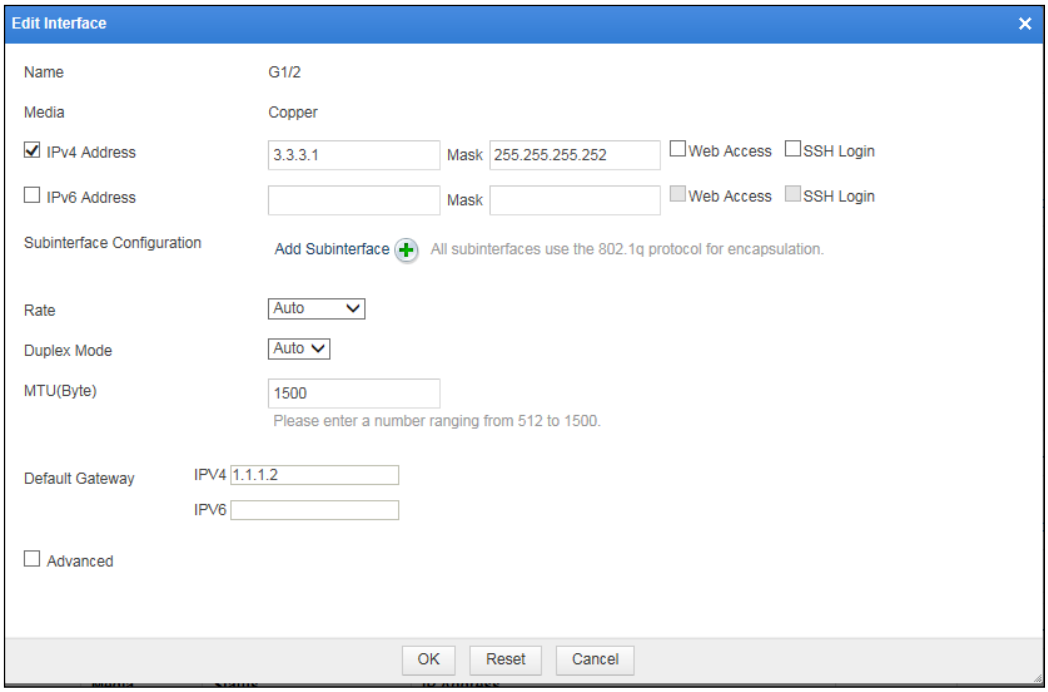
Figure 3-33 One-arm layer 3 injection — new work group on the Work Group Management page



Step 2 Configure the interface.

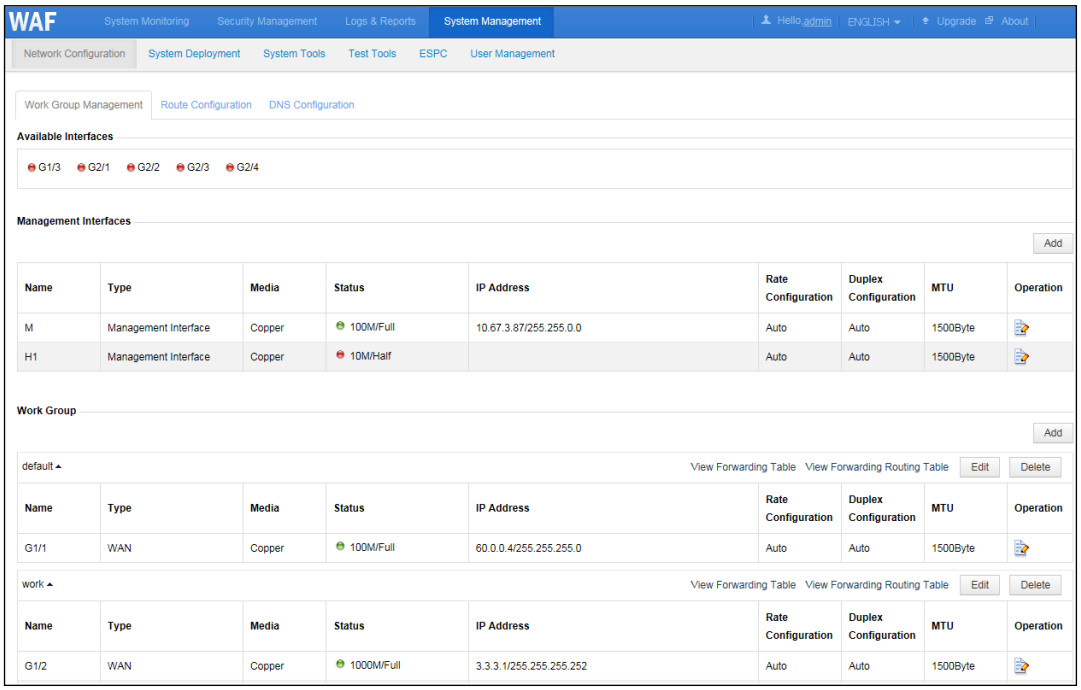
a. In the work group table shown in Figure 3-33, click in the row of interface G1/2 to edit interface parameters in the **Edit Interface** dialog box, as shown in Figure 3-34.

Figure 3-34 One-arm layer 3 injection — editing interface configuration



b. Click **OK** to complete the configuration and return to the **Work Group Management** page, as shown in Figure 3-35.

Figure 3-35 One-arm layer 3 injection — interface configuration

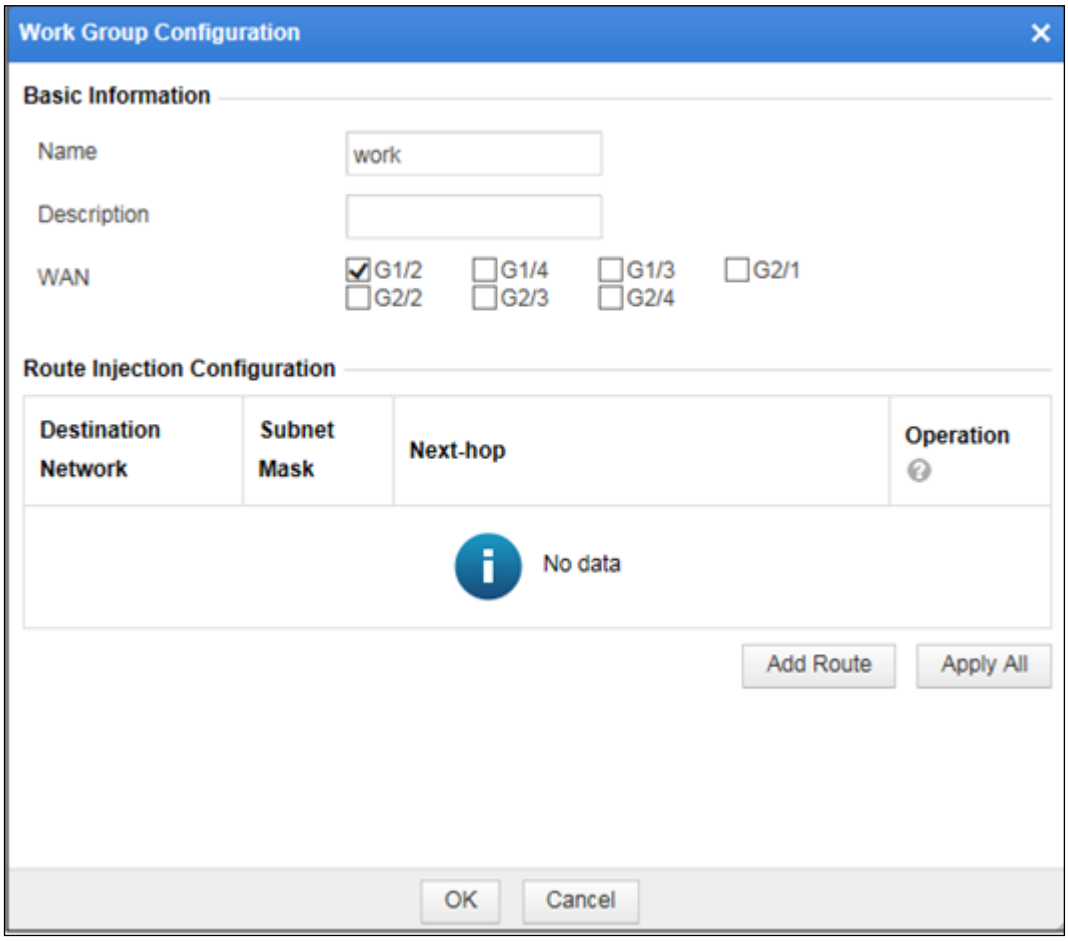


Configuring an Injection Route

Step 1 On the **Work Group Management** page shown in Figure 3-35, click **Edit** in the upper-right corner of the work group table.

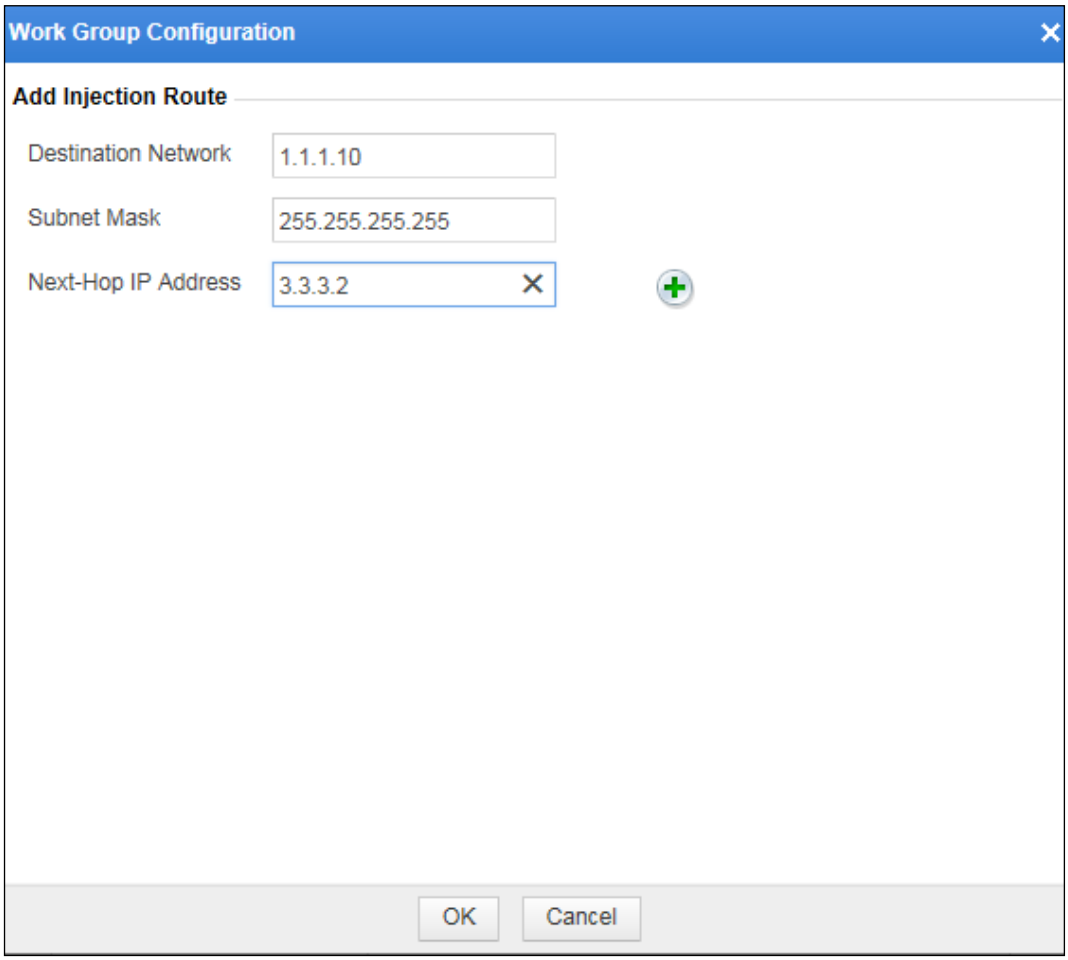
The **Work Group Configuration** dialog box appears, as shown in Figure 3-36.

Figure 3-36 One-arm layer 3 injection — editing a work group



Step 2 In the lower-right corner of the injection route list, click **Add Route** to add an injection route, as shown in Figure 3-37.

Figure 3-37 One-arm layer 3 injection — adding an injection route



Note	**Destination Network** (1.1.1.10) is the IP address of the server, and **Next-Hop IP Address** (3.3.3.2) is the IP address of the injection interface on the switch directly connected to WAF.

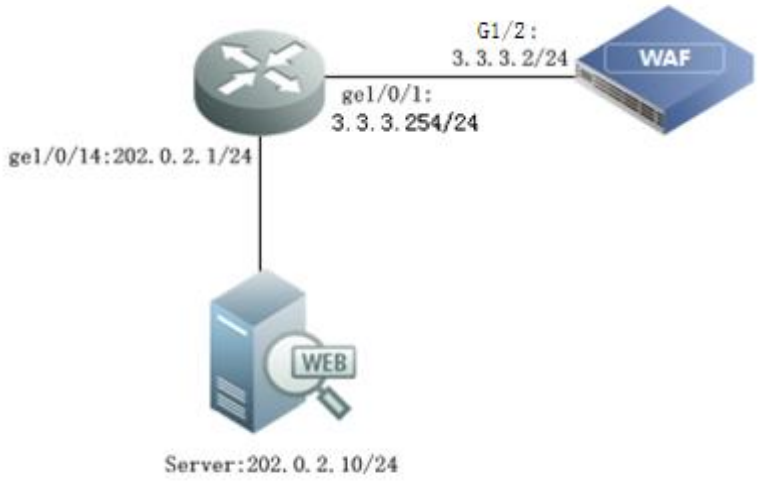
Step 3 Click **OK** to complete the configuration.

----End

3.2 One-Arm Traditional Reverse Proxy

Figure 3-38 shows the one-arm traditional reverse proxy topology of WAF.

Figure 3-38 One-arm traditional reverse proxy — topology



Router Configuration

Configuration Command	Description
interface GigabitEthernet1/0/1 description Connect-To-WAF no switchport ip address 3.3. 3.254 255.255.255.0 !	These commands configure an interface used by the router to connect to a WAN interface on WAF.
interface GigabitEthernet1/0/14 description Connect-To-Service no switchport ip address 202.0.2.1 255.255.255.0 !	These commands configure an interface used by the router to connect to the server.

WAF Configuration

Note	The IP address of a WAN interface on WAF is configured as the proxied IP address.

Configuring a Reverse Proxy Interface

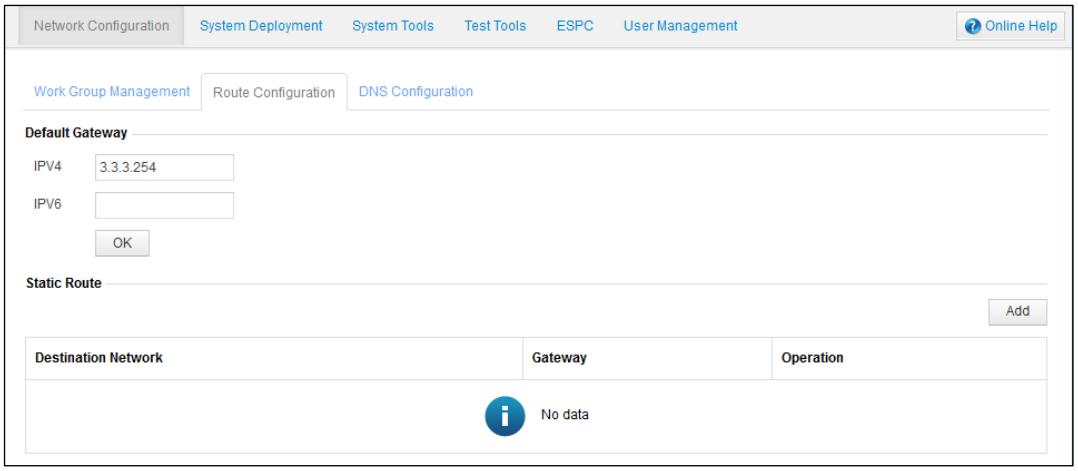
A reverse proxy interface is configured in the same way as the interface configured in one-arm layer 3 injection mode. For details, see Configuring the Interface in section 3.1.4.3 One-Arm Layer 3 Injection.

Configuring the Default Route

Step 1 Choose **System Management** > **Network Configuration** > **Route Configuration**.

The **Route Configuration** page appears. Change the IP address of the default gateway to **3.3.3.254**, as shown in Figure 3-39**.**

Figure 3-39 One-arm traditional reverse proxy — configuring the default route



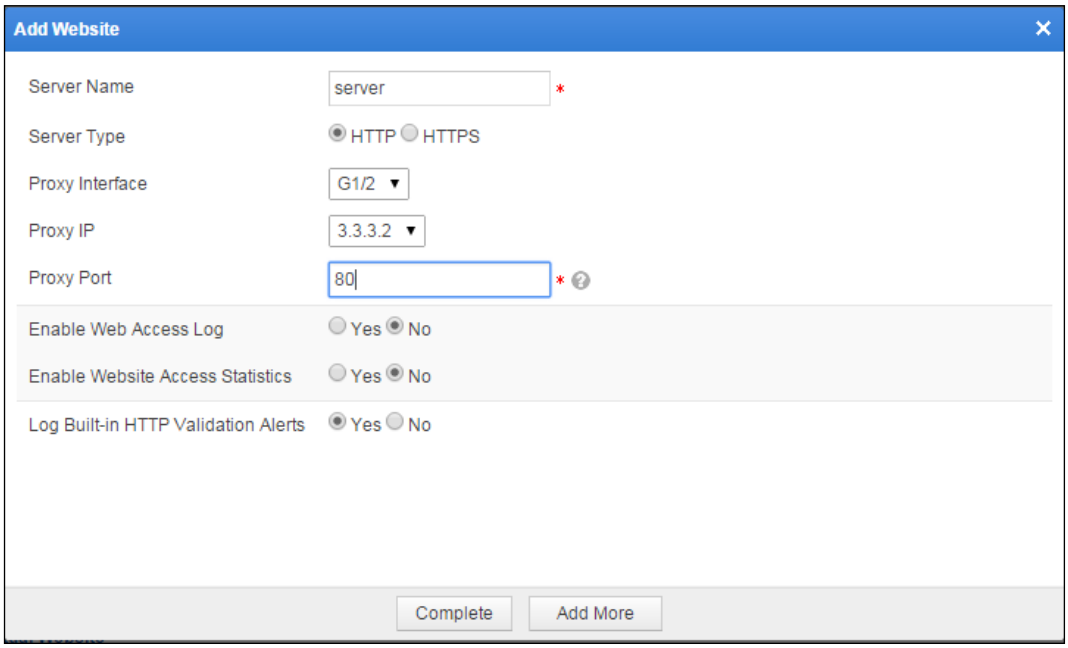
Step 2 Click **OK** to complete the configuration.

----End

Configuring the Proxied Server

Step 1 In reverse proxy mode, when adding a website, configure the proxied server and parameters of the proxy server and proxied server, as shown in Figure 3-40.

Figure 3-40 One-arm traditional reverse proxy — adding a website



Step 2 Click **Complete** to complete the configuration.

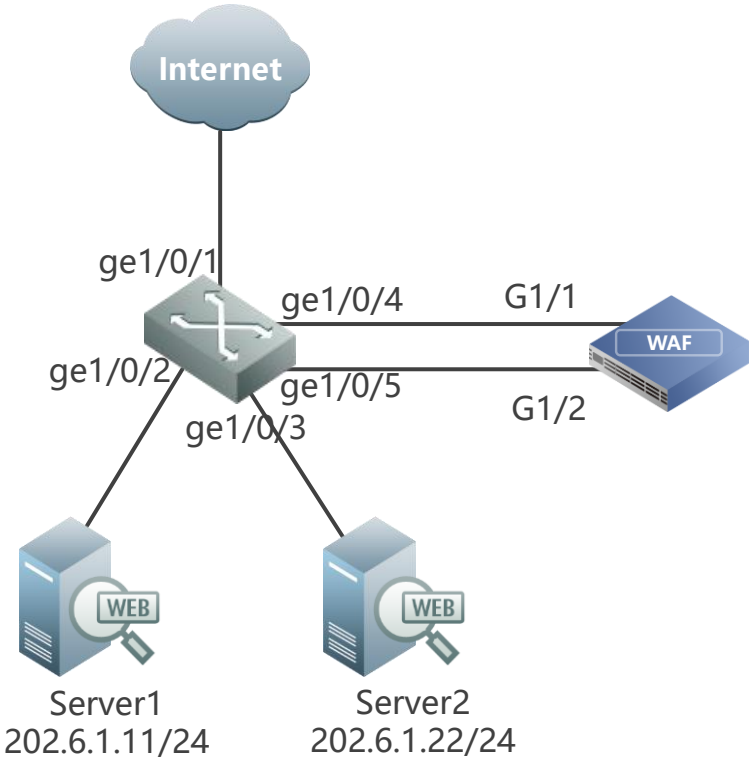
----End

3.3 Mirroring Deployment

In the mirroring deployment topology of WAF shown in Figure 3-41, interfaces G1/1 and G1/2 on WAF and ge1/0/4 and ge1/0/5 on the switch are mirroring interfaces.

- Interface ge1/0/4 serves as a mirroring interface of the switch and connects to interface G1/1 of WAF. It is used to mirror data traffic between interface ge1/0/2 and Server1.
- Interface ge1/0/5 serves as the other mirroring interface of the switch and connects to interface G1/2 of WAF. It is used to mirror data traffic between interface ge1/0/3 and Server2.

Figure 3-41 Mirroring deployment topology



Legend:

- ge1/0/1: connects to the Internet.
- ge1/0/2: 10.67.1.101/24, connects to Server1.
- ge1/0/3: 202.6.1.202/24, connects to Server2.

Switch Configuration

Configuration Command	Description
interface GigabitEthernet1/0/2 description Connect-To-Service no switchport ip address 202.6.1.11 255.255.255.0 !	Connects Server1.
interface GigabitEthernet1/0/3 description Connect-To-Service no switchport ip address 202.6.1.22 255.255.255.0 !	Connects Server2.
monitor session 1 source interface GigabitEthernet1/0/2	Mirrors data of interface ge1/0/2 to

Configuration Command	Description
monitor session 1 destination interface GigabitEthernet1/0/4	interface ge1/0/4.
monitor session 2 source interface GigabitEthernet1/0/3 monitor session 2 destination interface GigabitEthernet1/0/5	Mirrors data of interface ge1/0/3 to interface ge1/0/5.

WAF Configuration

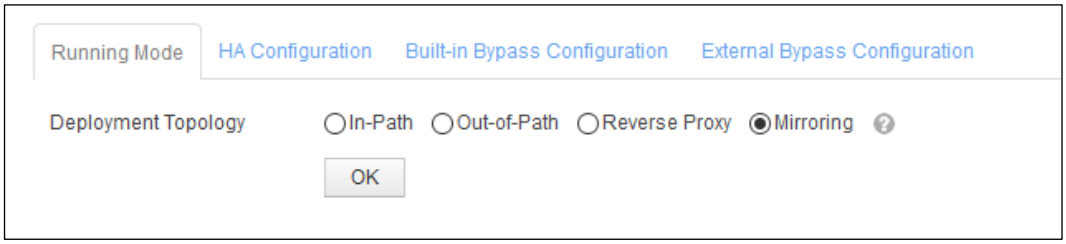
Step 1 Configure the deployment mode of WAF.

a. Log in to the web-based manager of WAF.

b. Choose **System Management > System Deployment > Running Mode**.

c. Set **Deployment Topology** to **Mirroring** and click **OK**.

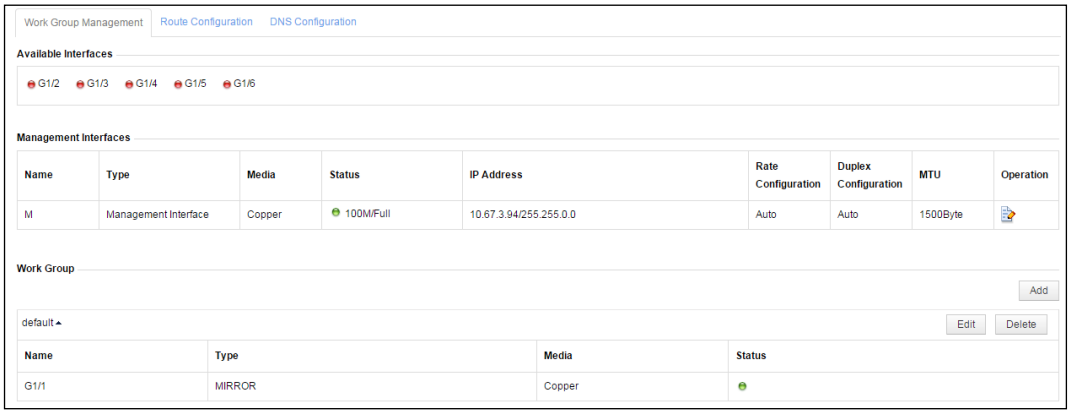
Figure 3-42 Running Mode page



Step 2 Configure the mirroring interface.

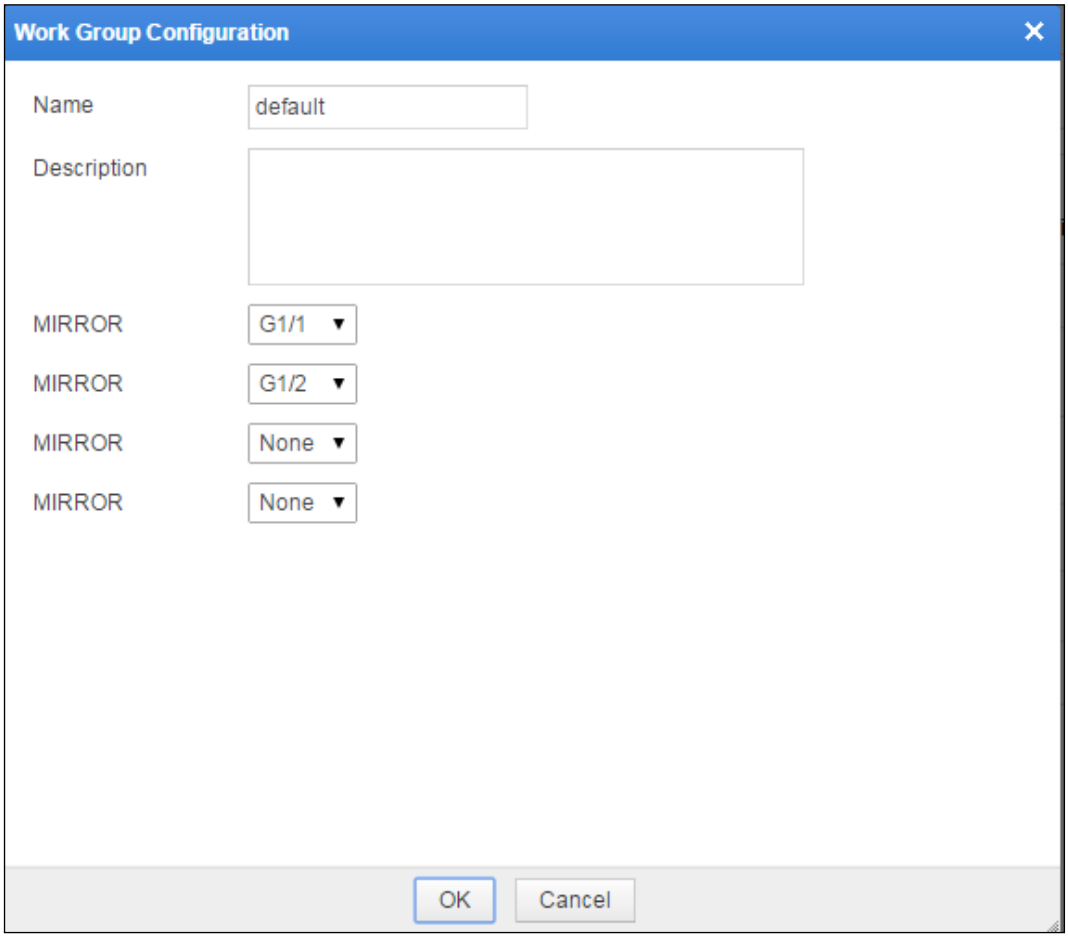
a. Choose **System Management > Network Configuration > Work Group Management**.

Figure 3-43 Mirroring mode — Work Group Management page



b. Click **Edit** in the upper-right corner of the **Work Group** area and then add the mirroring interface G1/2. Interface G1/1 is the default mirroring interface. See Figure 3-44.

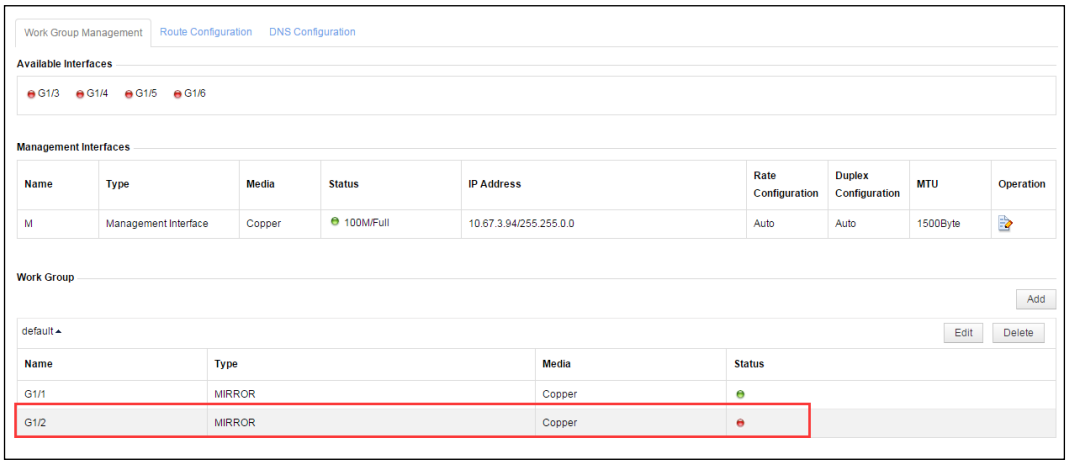
Figure 3-44 Editing mirroring interfaces



c. Click **OK** to save the settings.

G1/2 is added and displayed on the **Work Group Management** page in the **default** work group. See Figure 3-45.

Figure 3-45 New mirroring interface



----End

4 HA Configuration

This chapter describes WAF's HA deployment in the following in-path modes:

- Active-Active Mode via Port Channel
- Active-Active Mode via OSPF
- Master/Slave Mode

4.1 Active-Active Mode via Port Channel

Scenario

In the network environment shown in Figure 4-1, two WAFs (WAF A and WAF B) are deployed, and switch 1 (SW1) and switch 2 (SW2) are connected via a port channel.

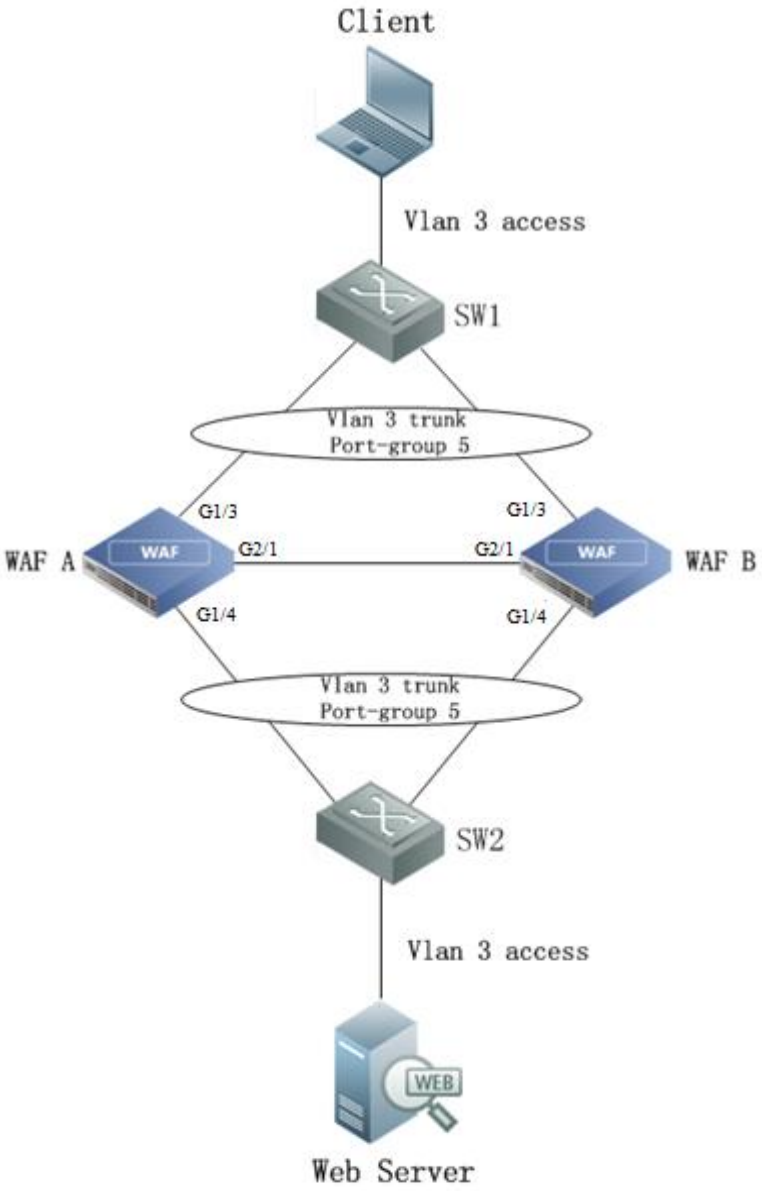
As SW1 and SW2 adopt different load balancing algorithms, asymmetrical traffic occurs when the client accesses the web server, that is, the client's request and the server's response are transmitted along different paths. Network disconnection may occur in the following process:

- A client request reaches the server after passing through SW1, WAF A, and SW2.
- A server response to the request reaches WAF B after passing through SW2.

This is because WAF B cannot find the corresponding session and discards the response.

To ensure smooth network communication, the HA active-active mode is configured on both WAFs in this scenario.

Figure 4-1 Active-active mode via port channel — topology



Preparation

Prepare the following:

- Two WAFs that can ping each other.
- Administrator account **admin**.

Configuration Roadmap

The configuration roadmap is as follows:

1. Perform the following configuration on both WAF A and WAF B as administrator **admin**:

- Enable HA, set the working mode, and configure the HA interface.
- Create a work group and specify the WAN interface and LAN interface.

2. Verify the configuration result.

----End

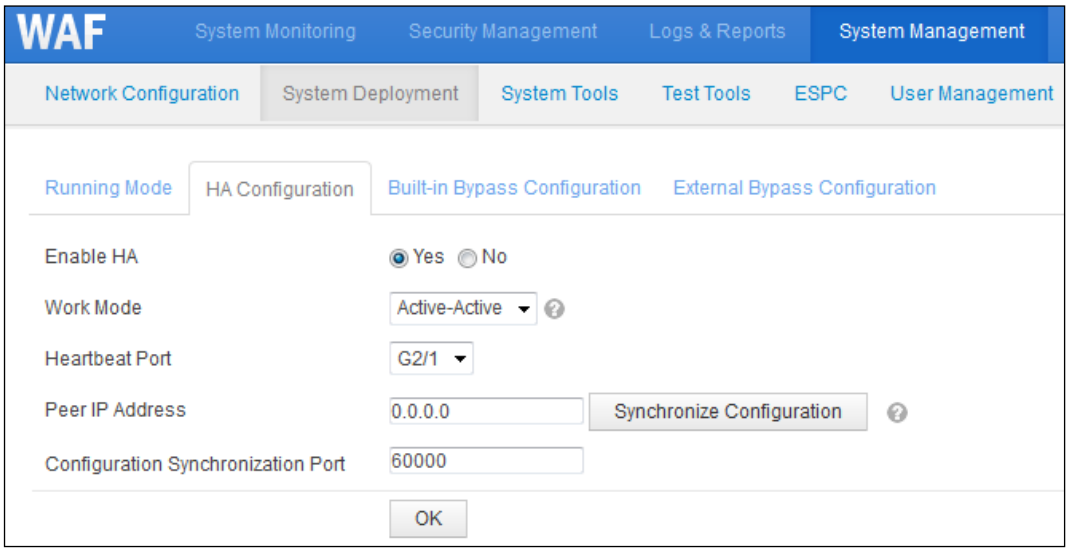
Configuration Procedure

Perform the following steps to configure HA on WAF A and WAF B as administrator **admin**:

Step 1 Perform the HA configuration on WAF A.

Choose **System Management** > **System Deployment** > **HA Configuration**. On the **HA Configuration** page that is displayed shown in Figure 4-2, select the **Enable HA** check box, set **Work Mode** to **Active-Active**, and click **OK**.

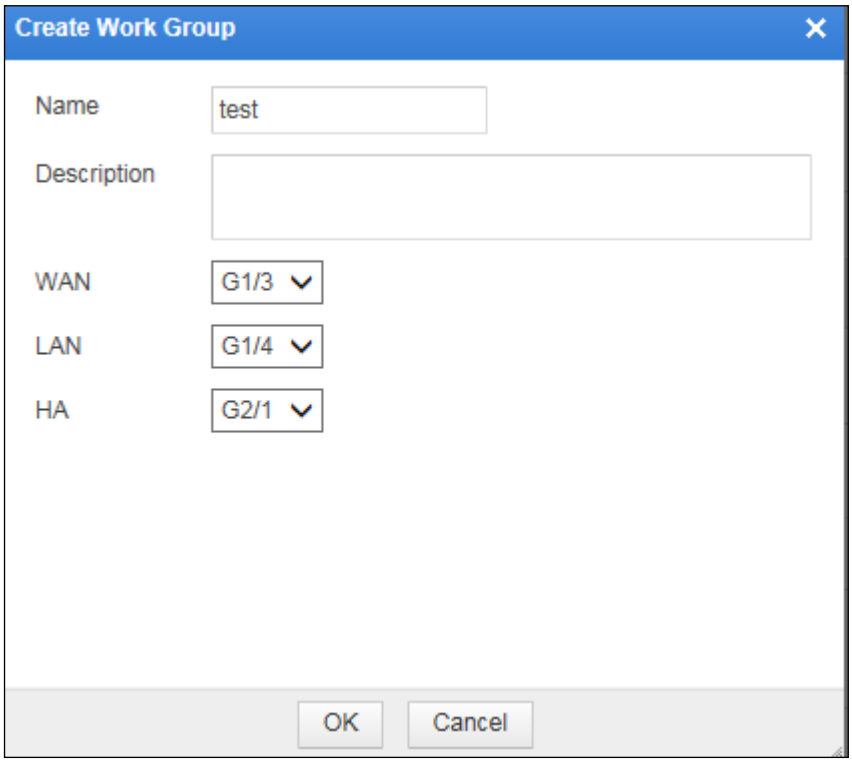
Figure 4-2 Active-active mode via port channel — HA configuration



Step 2 Create a work group on WAF A.

Choose **System Management** > **Network Configuration** > **Work Group Management**. On the **Work Group Management** page that is displayed, click **Add** to add a work group, for example, **test**, as shown in Figure 4-3.

Figure 4-3 Active-active mode via port channel — creating a work group



Step 3 Repeat steps 1 and 2 on WAF B to perform the same configuration.

----End

Verification

After the preceding configurations are completed, smooth network communication is ensured in the following process:

- A client request reaches the server after passing through SW1, WAF A, and SW2.
- A server response to the request reaches WAF B after passing through SW2.

This is because WAF B forwards the response to WAF A via the HA (G2/1) interface, and WAF A forwards the response to the client through SW1. The pair of request and response is transmitted along the same path.

4.2 Active-Active Mode via OSPF

Scenario

In the network environment shown in Figure 4-4, two WAFs (WAF A and WAF B) are deployed and three routers (R1, R2, and R3) belong to OSPF area 100. R3 announces that the routes from both R1 and R2 to the network segment where the web server resides have the same cost, that is, the two routes are equivalent. Also, R3 learns that routes from R1 and R2 to the client are equivalent.

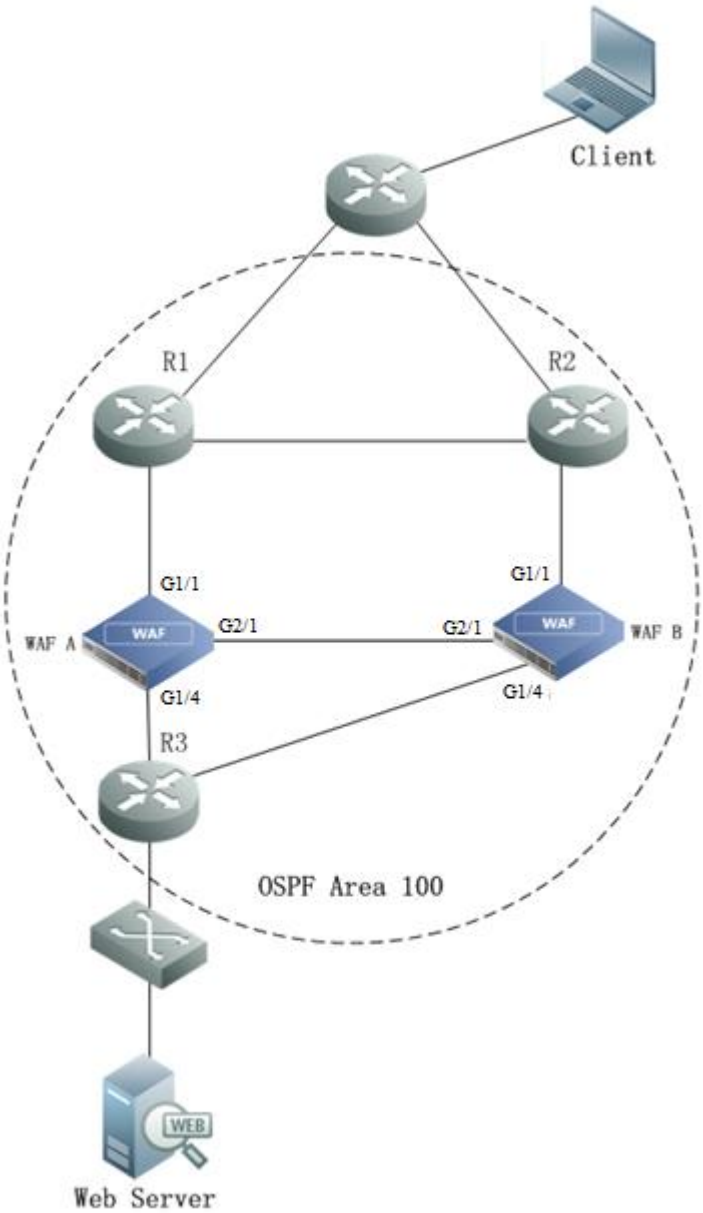
When the client accesses the web server, asymmetrical traffic occurs, that is, the client's request and the server's response are transmitted along different paths. Network disconnection may occur in the following process:

- A client request reaches the server after passing through R1, WAF A, and R3.
- A server response to the request reaches WAF B after passing through R3.

This is because WAF B cannot find the corresponding session and discards the response.

To ensure smooth network communication, the HA active-active mode is configured on two WAFs.

Figure 4-4 Active-active mode via OSPF — topology



Note	For the preceding topology, assume the following: • The IP address of the default gateway of WAF A is 10.30.255.254. • The peer MAC address of interface G1/1 on WAF A is 5C-F9-DD-73-94-DE. • The IP address of the default gateway of WAF B is 10.31.255.254. • The peer MAC address of interface G1/1 on WAF B is 5C-F9-DE-53-62-AE.

Preparation

Prepare the following:

- Two WAFs that can ping each other.
- Administrator account **admin.**

Configuration Roadmap

The configuration roadmap is as follows:

1. Perform the following configuration on both WAF A and WAF B as administrator **admin**:
   - Enable HA and set the working mode.
   - Create a work group and specify the WAN interface, LAN interface, and HA interface.
   - Edit the configuration of interface G1/1 in the work group and bind the peer MAC address.
2. Verify the configuration result.

----End

Configuration Procedure

Step 1 Perform HA configuration and create a work group named **test** by repeating Step 1 to Step 3 in Configuration Procedure in section 4.1 Active-Active Mode via Port Channel.

Step 2 Edit the configuration in interface G1/1 in the new work group in WAF A.

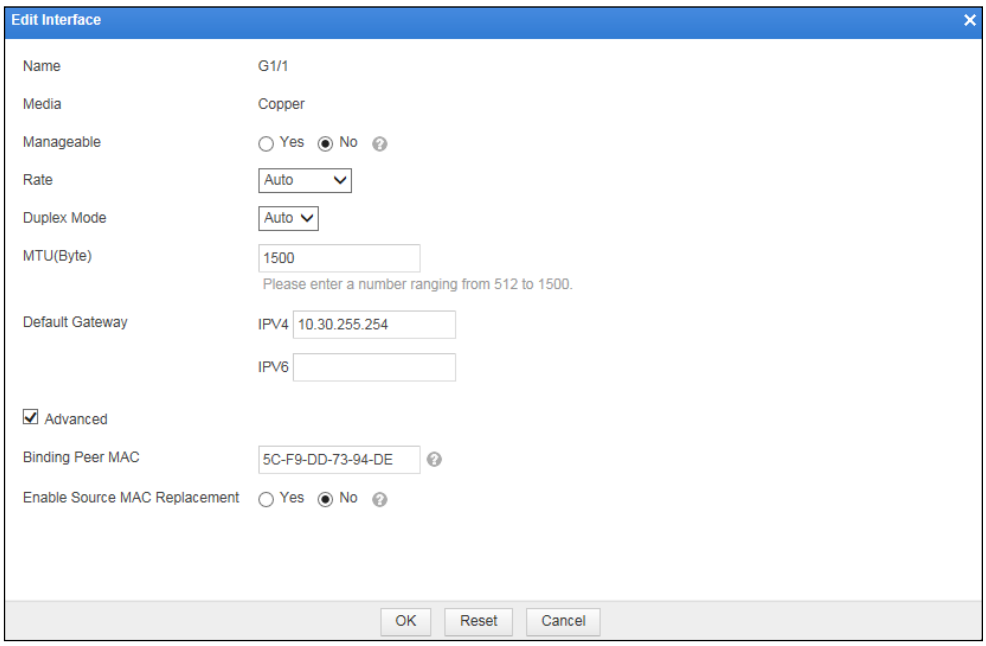
a. Choose **System Management** > **Network Configuration** > **Work Group Management**.

b. On the **Work Group Management** page, click in the row of interface G1/1 on the table of the work group **test**.

c. Edit interface configuration in the displayed **Edit Interface** dialog box, as shown in Figure 4-5.

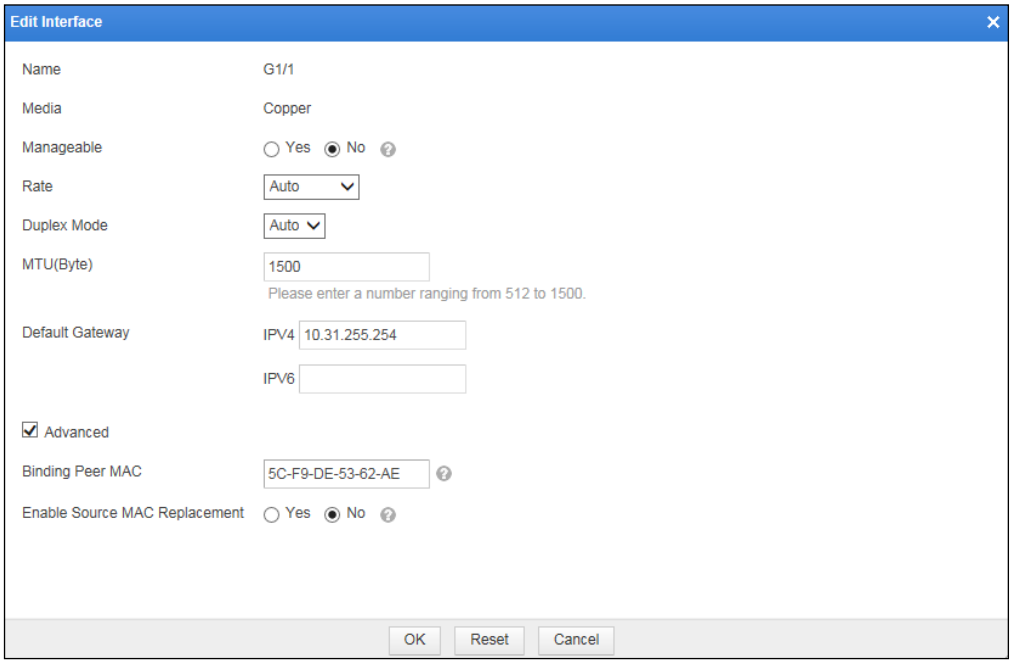
d. Click **OK** to complete the configuration.

Figure 4-5 Active-active mode via OSPF — editing interface G1/1 configuration in the work group on WAF A



Step 3 Repeat Step 2 to edit interface G1/1 configuration on WAF B.

Figure 4-6 Active-active mode via OSPF — editing interface G1/1 configuration in the work group on WAF B



----End

Verification

After the preceding configurations are completed, smooth network communication is ensured in the following process:

- A client request reaches the server after passing through R1, WAF A, and R3.
- A server response to the request reaches WAF B after passing through R3.

This is because WAF B forwards the response to WAF A via the HA (G2/1) interface, and WAF A forwards the response to the client through R1. The pair of request and response is transmitted along the same path.

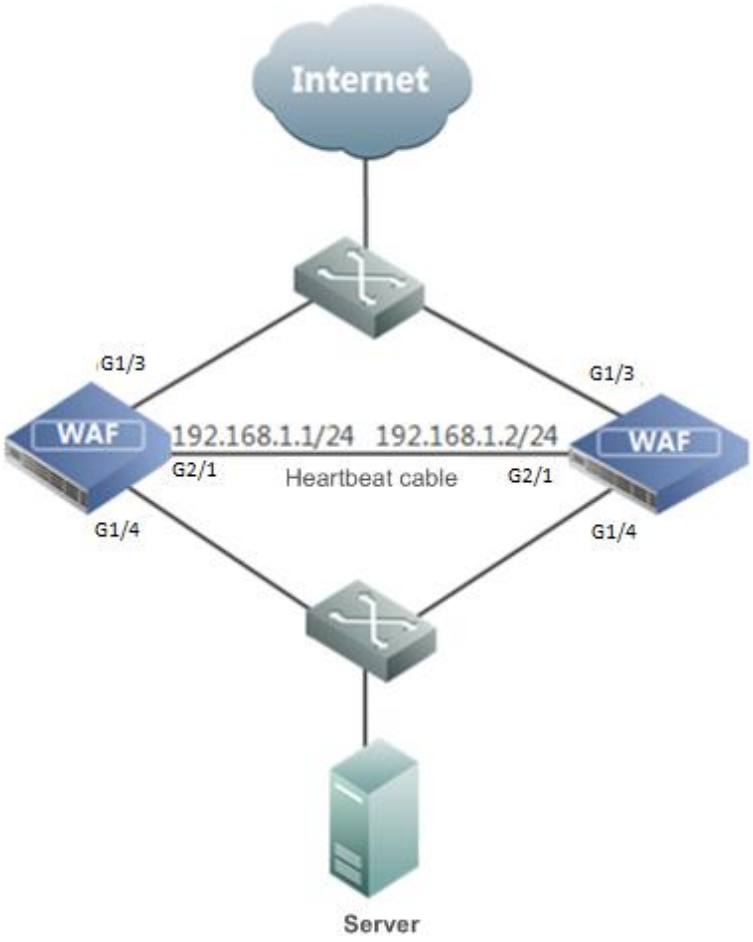
4.3 Master/Slave Mode

Two WAFs can work in master/slave mode to meet the security protection requirement of a network where redundant links are available, implementing hot standby. In master/slave mode, once the master WAF fails, the slave WAF takes over all traffic from the master WAF to ensure proper network communication.

Scenario

Each of the master and slave WAFs has a pair of interfaces to connect to switches on both ends. The two WAFs connect to each other via a working interface (heartbeat interface) that is used to exchange heartbeat information and synchronize configuration files and session information. The working interfaces on the master WAF are in Up state, through which network traffic is transmitted. The working interfaces on the slave WAF is in Down state, acting as standby interfaces for traffic transmission. Figure 4-7 shows the master/slave topology.

Figure 4-7 Master/Slave mode — topology



Preparation

Prepare two WAFs, each with three working interfaces. Among the three interfaces, two (G1/3 and G1/4 in group1) are used to connect to switches, forward data, and perform failover; the other (G2/1) serves as the heartbeat interface.

Caution	• In master/slave mode, the model and software version of the master and slave WAFs must be the same. Otherwise, the synchronization configuration may fail. • The two WAFs usually use a working interface, rather than the default management interface, as the heartbeat interface to connect to each other. • Switches that are connected to both ends of WAFs must be in the same VLAN.

Configuration Roadmap

Perform the following configuration on both the master and slave WAFs:

1. Configure working interfaces.
2. Configure HA parameters.
3. Synchronize configuration files.

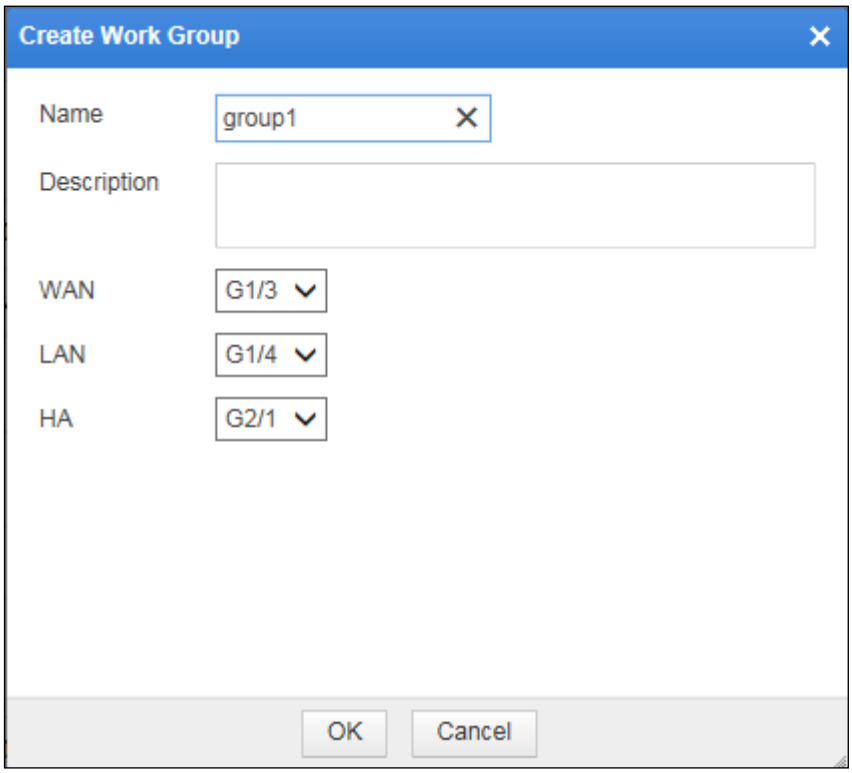
Configuration Procedure

Step 1 Configure working interfaces on both the master and slave WAFs:

a. Choose **System Management** > **Network Configuration** > **Work Group Management**.

b. On the **Work Group Management** page that appears, click **Add** in the lower-right corner of the **Work Group** area to add a work group by setting **Name** to **group1**, **WAN** to **G1/3**, **LAN** to **G1/4**, **HA** to **G2/1**, and leaving **Description** blank, as shown in Figure 4-8.

Figure 4-8 Master/Slave mode — adding a work group



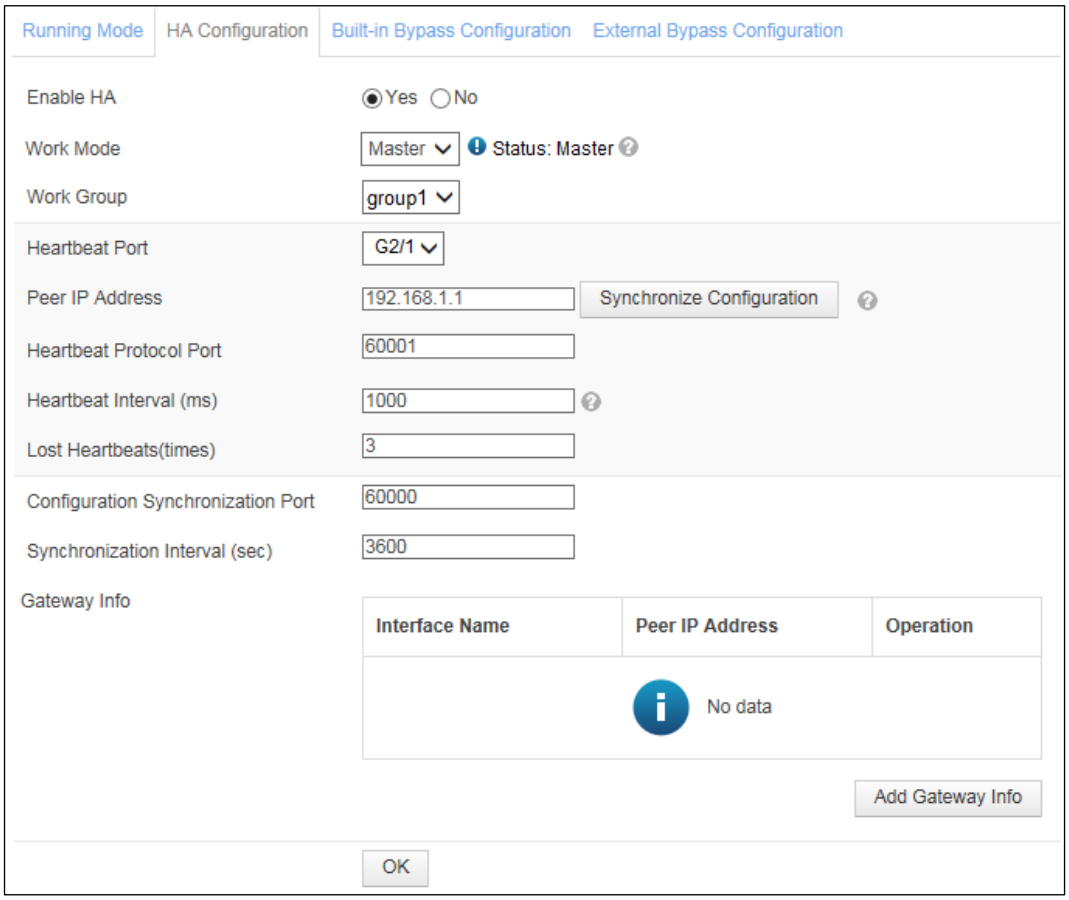
c. Click **OK** to complete the configuration.

Step 2 Configure HA parameters on both WAFs.

On both WAFs, choose **System Management** > **System Deployment** > **HA Configuration**. The **HA Configuration** page appears.

a. On the master WAF, select the **Enable HA** check box, set **Work Mode** to **Master**, **Work Group** to **group1**, **Heartbeat Port** to **G2/1**, **Peer IP Address** to **192.168.1.1**, and leave other parameters at their default values, as shown in Figure 4-9.

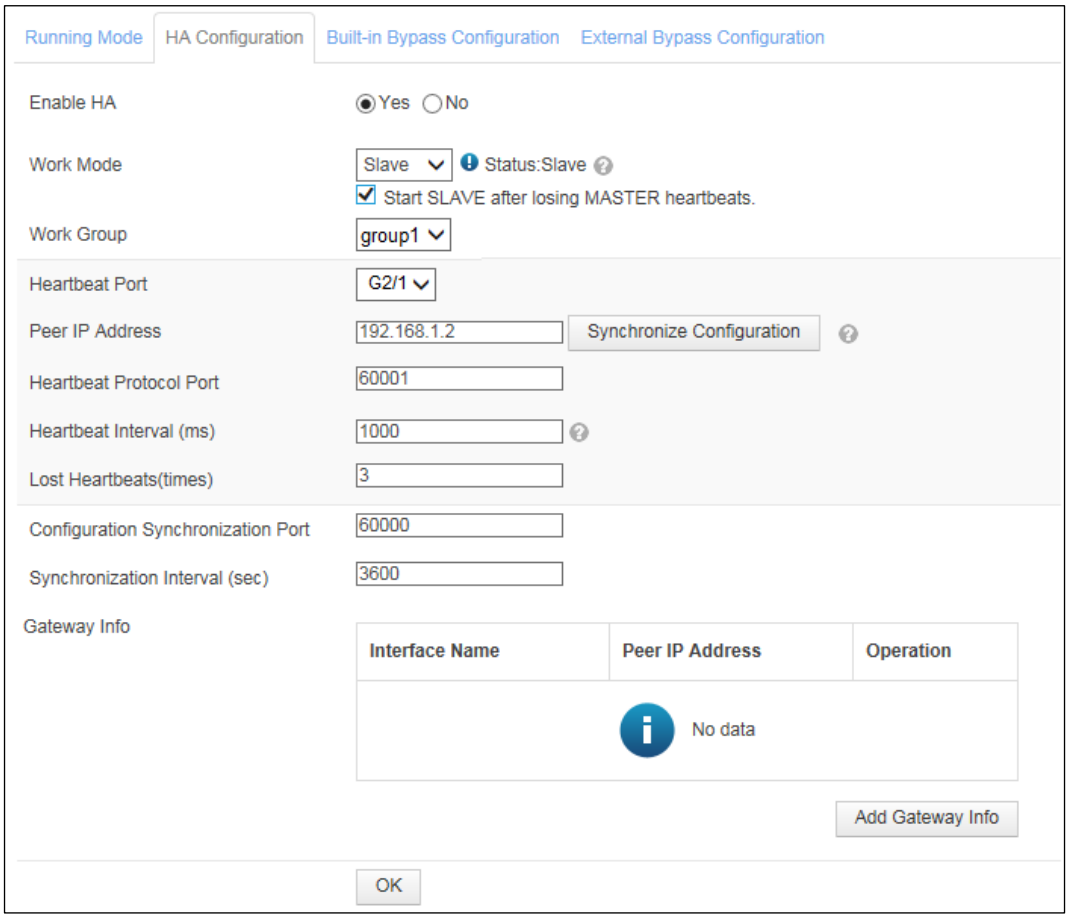
Figure 4-9 Master/Slave mode — HA configuration on the master WAF



b. Click **OK** to complete the configuration.

c. On the slave WAF, select the **Enable HA** check box, set **Work Mode** to **Slave**, **Work Group** to **group1**, **Heartbeat Port** to **G2/1**, **Peer IP Address** to **192.168.1.2**, and leave other parameters at their default values, as shown in Figure 4-10.

Figure 4-10 Master/Slave mode — HA configuration on the standby WAF



d. Click **OK** to complete the configuration.

Note	On the **HA Configuration** page on WAF, you are advised to select the check box preceding **Start SLAVE after losing MASTER heartbeats** when configuring **Work Mode**.

Step 3 Synchronize configuration files between master and slave WAFs.

a. On the master WAF, choose **System Management** > **System Deployment** > **HA Configuration**.

b. On the **HA Configuration** page that appears, click **Synchronize Configuration** to synchronize configuration files from the master WAF to the slave WAF.

Step 4 Click **OK** to complete the configuration.

----End

Caution	In master/slave mode, the status is displayed as **Master** for the master WAF and **Slave** for the slave WAF. Once an working interface on the master WAF is down, all interfaces in the HA working group on the master WAF will be down, and the slave WAF takes traffic over from the master WAF. In this case, the status of the master WAF changes to **Slave**, and that of the slave WAF changes to **Master**.

5 VRRP Configuration

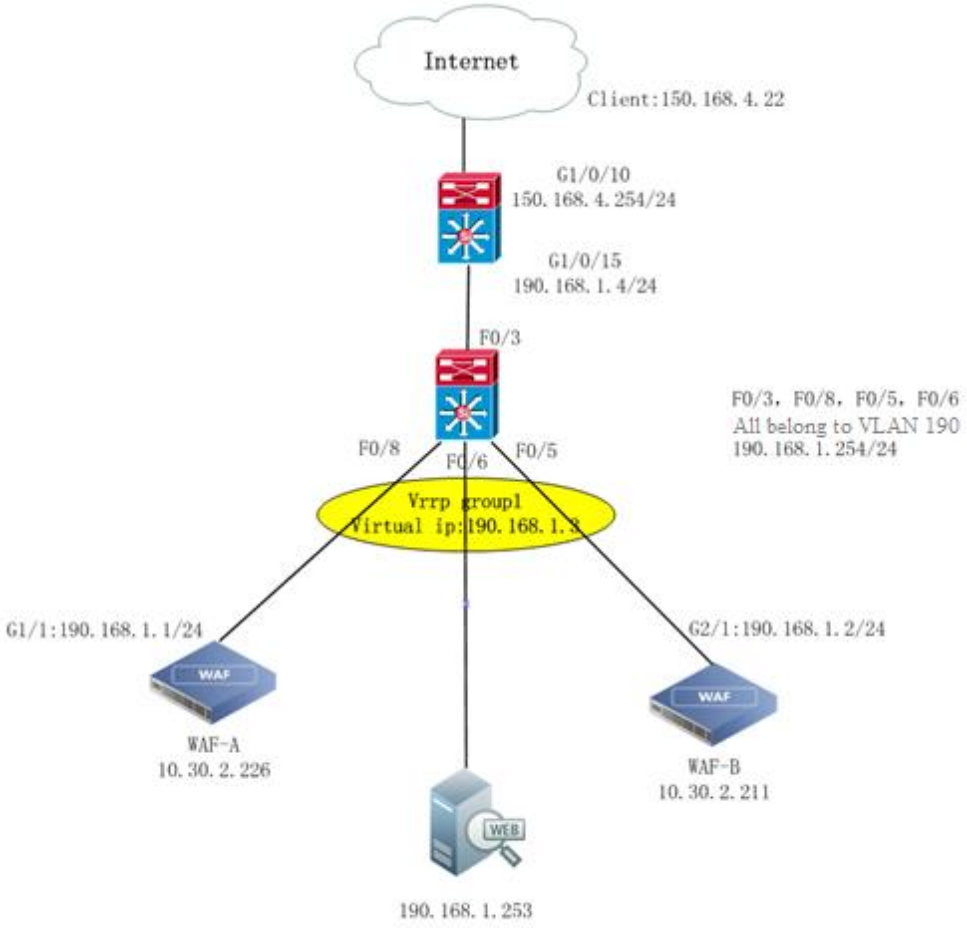
This chapter describes how to configure VRRP on WAFs deployed in reverse proxy mode.

5.1 Configuring a Single VRRP Group

Scenario

As shown in Figure 5-1, two WAFs are deployed on the network: WAF A and WAF B, which are in the same VRRP group. The virtual IP address and the IP addresses of the two WAFs are in the same network segment. To ensure uninterrupted network communications, it is necessary to configure VRRP on the two WAFs, one as the master and the other as the backup. In this manner, when the master WAF fails, the slave WAF automatically takes over traffic from the master WAF.

Figure 5-1 Deployment of WAFs in reverse proxy mode (a single VRRP group)



Preparation

Prepare the following:

- Two connected WAF devices
- Administrator account **admin**

Configuration Roadmap

The configuration roadmap is as follows:

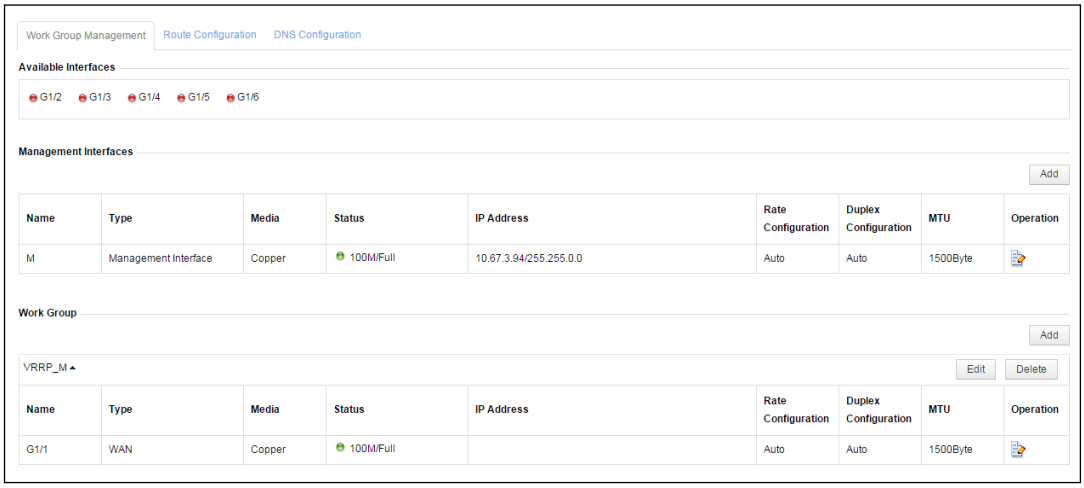
1. Perform the following configuration on both WAF A and WAF B as administrator **admin**:
   - Configure a working interface respectively on WAF A and WAF B.
   - Configure VRRP on WAF A and WAF B.
2. Verify the configuration.

Configuration Procedure on WAF A

Do as follows to configure VRRP on WAF A as administrator **admin**:

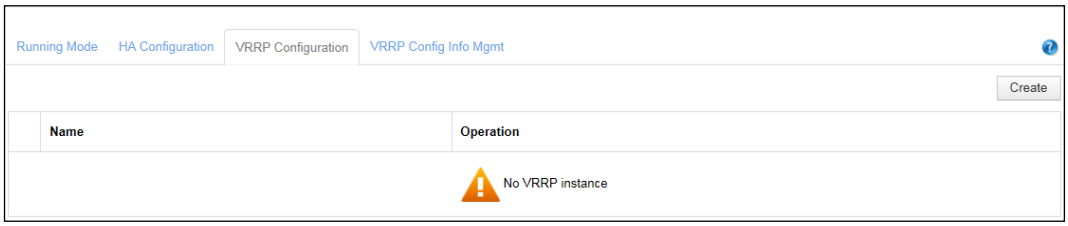
Step 1 Choose **System Management** > **Network Configuration** > **Work Group Management**. Specify a working interface, for example, G1/1, as shown in Figure 5-2.

Figure 5-2 Configuring working interface G1/1



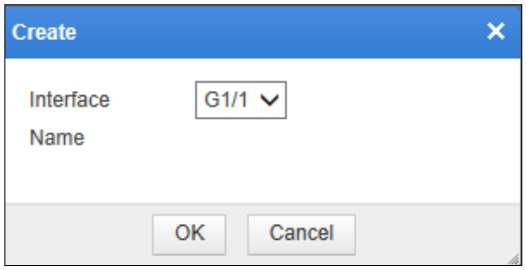
Step 2 Choose **System Management** > **System Deployment** > **VRRP Configuration**.

Figure 5-3 VRRP Configuration page



Step 3 Click **Create** to add interface G1/1.

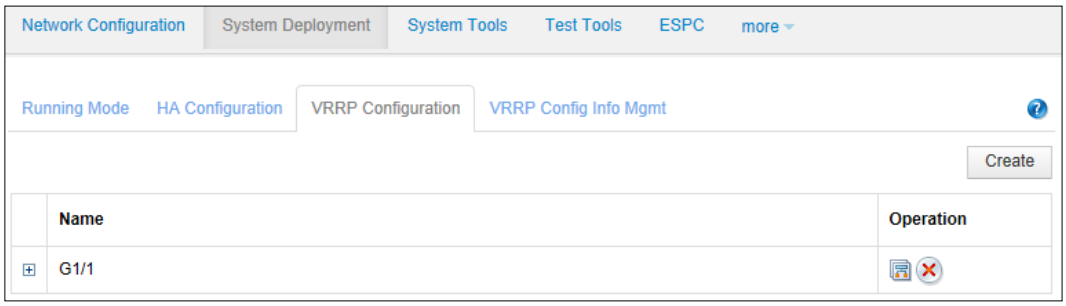
Figure 5-4 Adding interface G1/1



Step 4 Click **OK**.

Then interface G1/1 appears on the **VRRP Configuration** page, as shown in Figure 5-5.

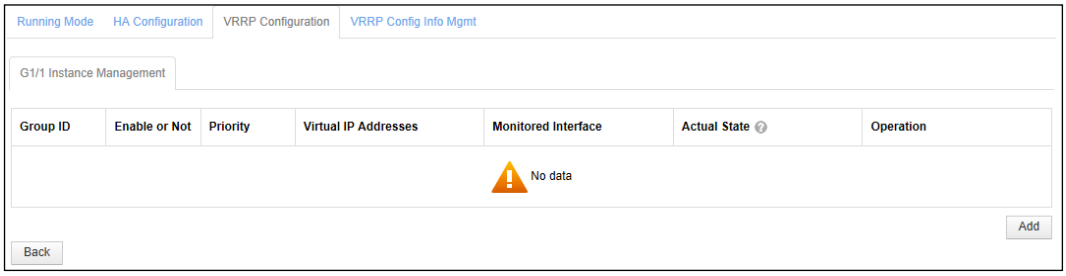
Figure 5-5 VRRP Configuration page after interface G1/1 is added



Step 5 Click the VRRP instance management icon in the **Operation** column of interface G1/1.

The **G1/1 Instance Management** page appears, as shown in Figure 5-6.

Figure 5-6 G1/1 Instance Management page

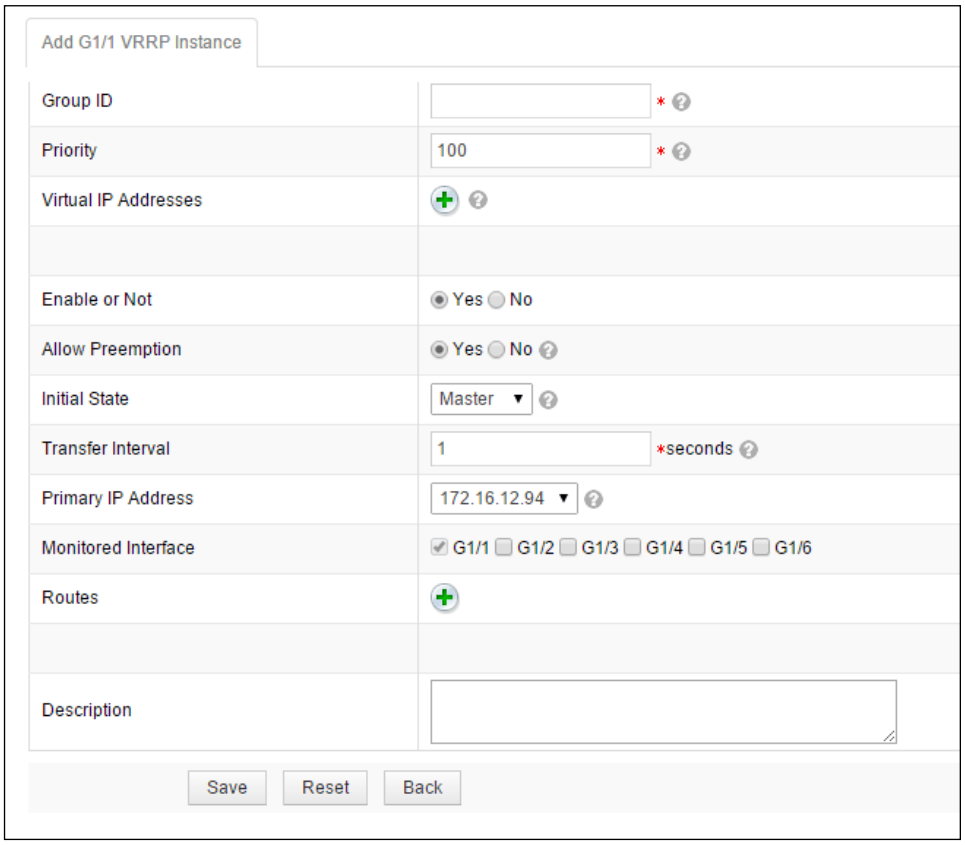


Step 6 Click **Add**.

The **Add G1/1 VRRP Instance** page appears, as shown in Figure 5-7.

Note	• VRRP instance parameters (such as **Group ID**, **Virtual IP Address**, and **Transfer Interval**) must be set to the same values on the master WAF and slave WAF. • When the virtual IP address and the server IP address are in different network segments, a route is required to ensure the connectivity between clients and the VRRP group.

Figure 5-7 G1/1 VRRP Instance Add page



Step 7 Configure parameters and click **Save** to commit the settings.

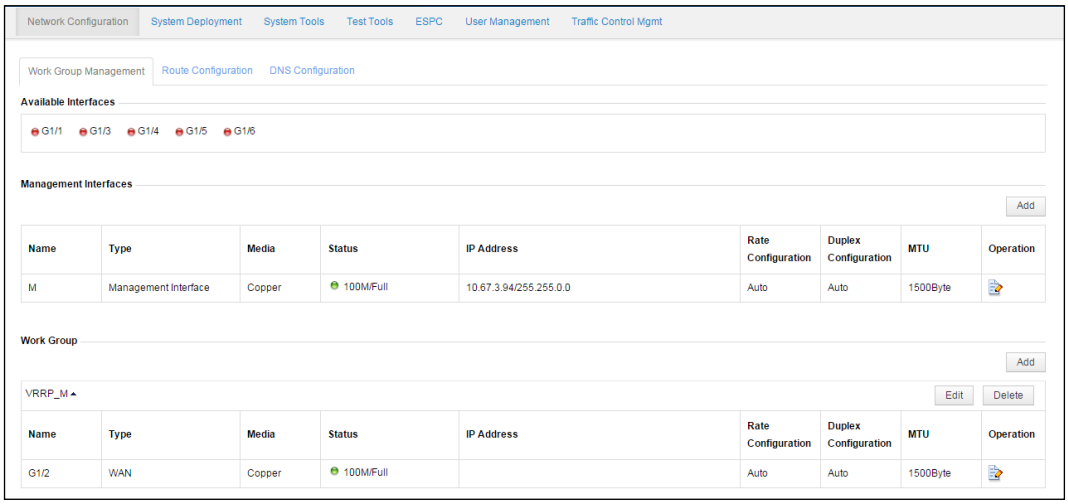
----End

Configuration Procedure on WAF B

Do as follows to configure VRRP on WAF B as administrator **admin**:

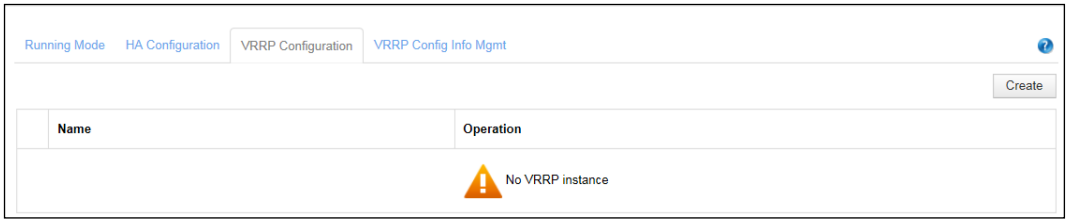
Step 1 Choose **System Management > Network Configuration > Work Group Management**. Specify a working interface, G1/2, as shown in Figure 5-8.

Figure 5-8 Configuring working interface G1/2



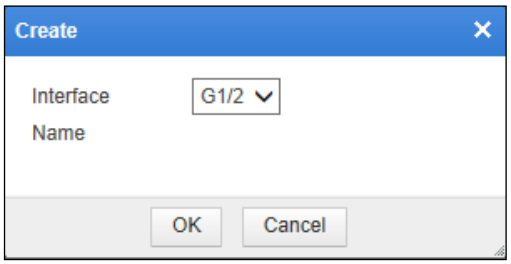
Step 2 Choose **System Management** > **System Deployment** > **VRRP Configuration**.

Figure 5-9 VRRP Configuration page



Step 3 Click **Create** to add interface G1/2.

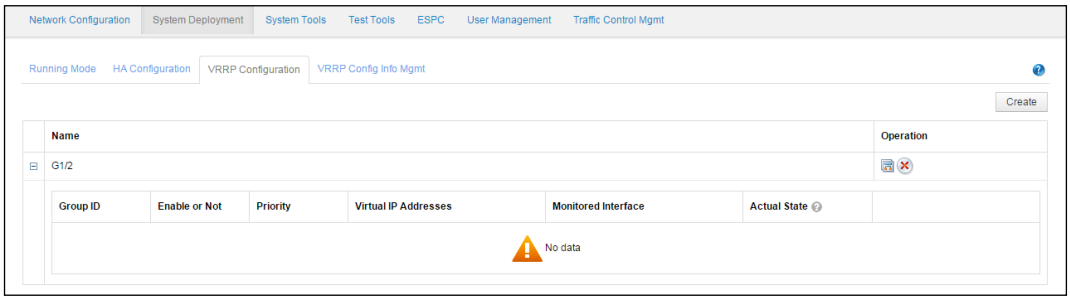
Figure 5-10 Adding interface G1/2



Step 4 Click **OK**.

Then interface G1/2 appears on the **VRRP Configuration** page, as shown in Figure 5-11.

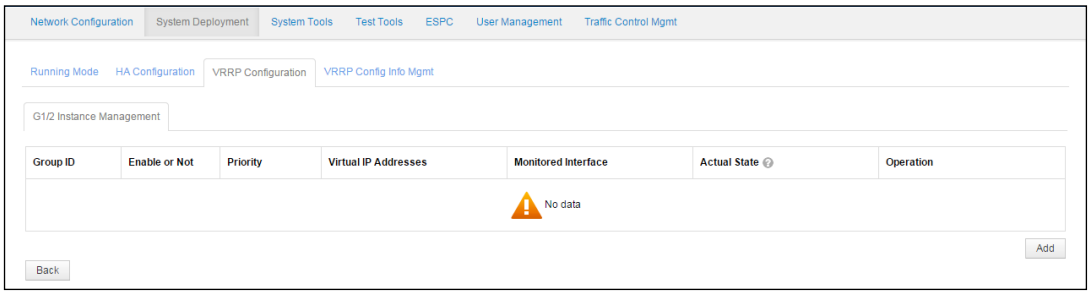
Figure 5-11 VRRP Configuration page after interface G1/2 is added



Step 5 Click the VRRP instance management icon in the **Operation** column of interface G1/2.

The **G1/2 Instance Management** page appears, as shown in Figure 5-12.

Figure 5-12 G1/2 Instance Management page

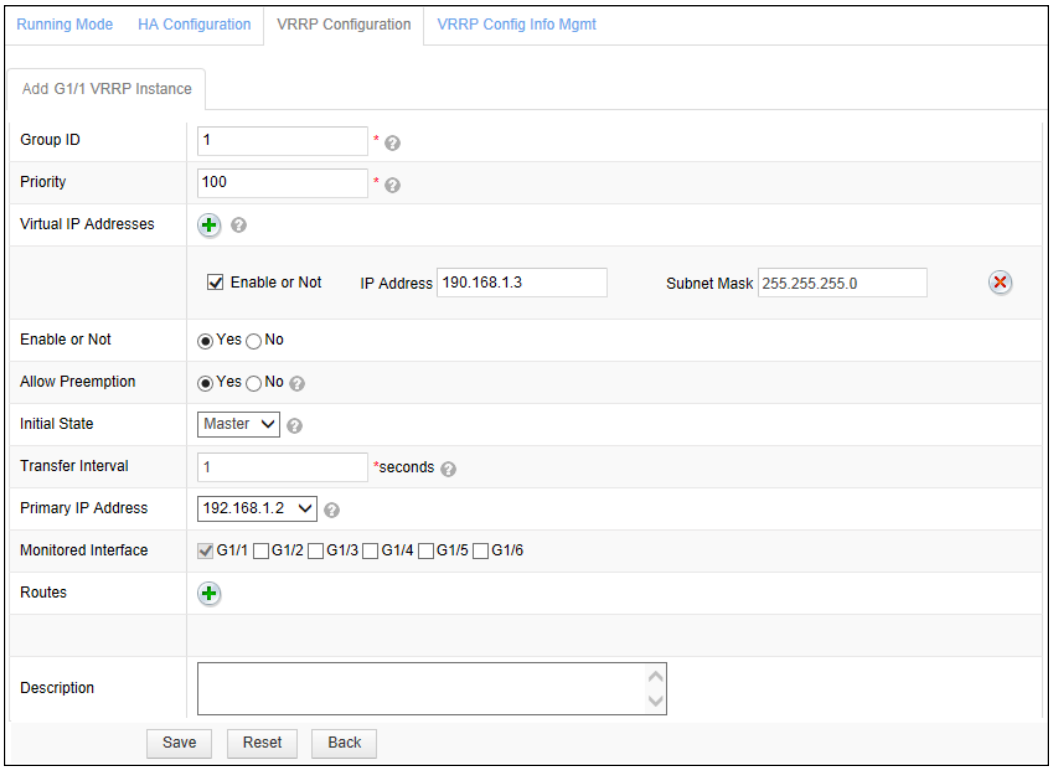


Step 6 Click **Add**.

The **Add G1/2 VRRP Instance** page appears, as shown in Figure 5-13.

Note	• VRRP instance parameters (such as **Group ID**, **Virtual IP Address**, and **Transfer Interval**) must be set to the same values on the master WAF and slave WAF. • When the virtual IP address and the server IP address are in different network segments, a route is required to ensure the connectivity between clients and the VRRP group.

Figure 5-13 G1/2 VRRP Instance Add page



Step 7 Configure parameters and click **Save** to commit the settings.

----End

Verification

After the preceding operations, WAF A and WAF B have been configured to negotiate with each other via VRRP. WAF A has a higher priority than WAF B, thus becoming the master device. Traffic from clients to the server is first diverted to WAF A for cleaning before reaching the destination.

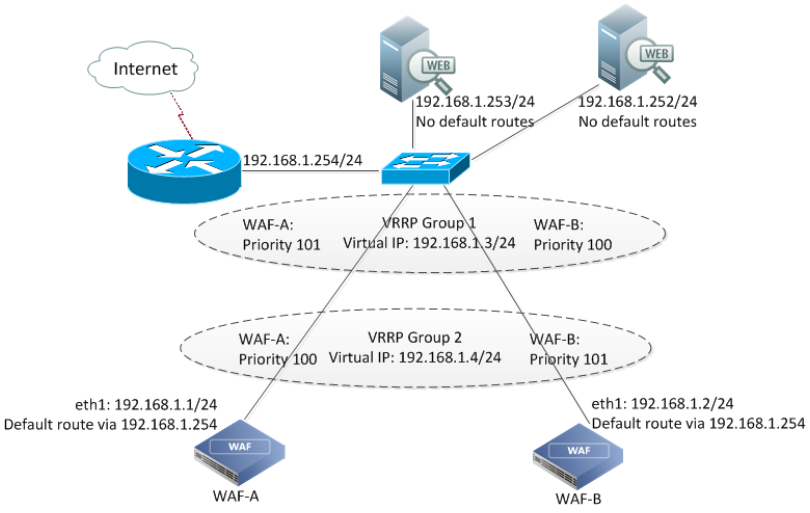
When the monitoring interface of WAF A, that is G1/1, fails, or WAF B cannot receive VRRP packets from WAF A, WAF B automatically switches to the active state. Then traffic from clients to the server is diverted to WAF B for cleaning. In this manner, network communications can proceed properly without being interrupted.

5.2 Configuring Multiple VRRP Groups

Scenario

As shown in Figure 5-14, two WAF devices are deployed on the network, with multiple VRRP instances configured. The two devices work in master/slave mode, jointly handling service traffic destined for servers. When the master device in a VRRP instance becomes faulty, the slave device will take over all the traffic, thereby ensuring business continuity.

Figure 5-14 Deployment of WAF devices in reverse proxy mode (multiple VRRP groups)



Preparation

Prepare the following:

- Two WAF devices (WAF A and WAF B) that interconnect with each other and connect to the same switch, working in reverse proxy mode
- Protected server, with one-to-many or many-to-many mapping between the domain name and IP address
- Administrator account **admin**

Configuration Roadmap

The configuration roadmap is as follows:

1. Perform the following configuration on both WAF A and WAF B as administrator **admin**:
   - Configure a working interface respectively on WAF A and WAF B.
   - Configure two VRRP instances respectively on WAF A and WAF B.
2. Verify the configuration.

Configuration Procedure on WAF A

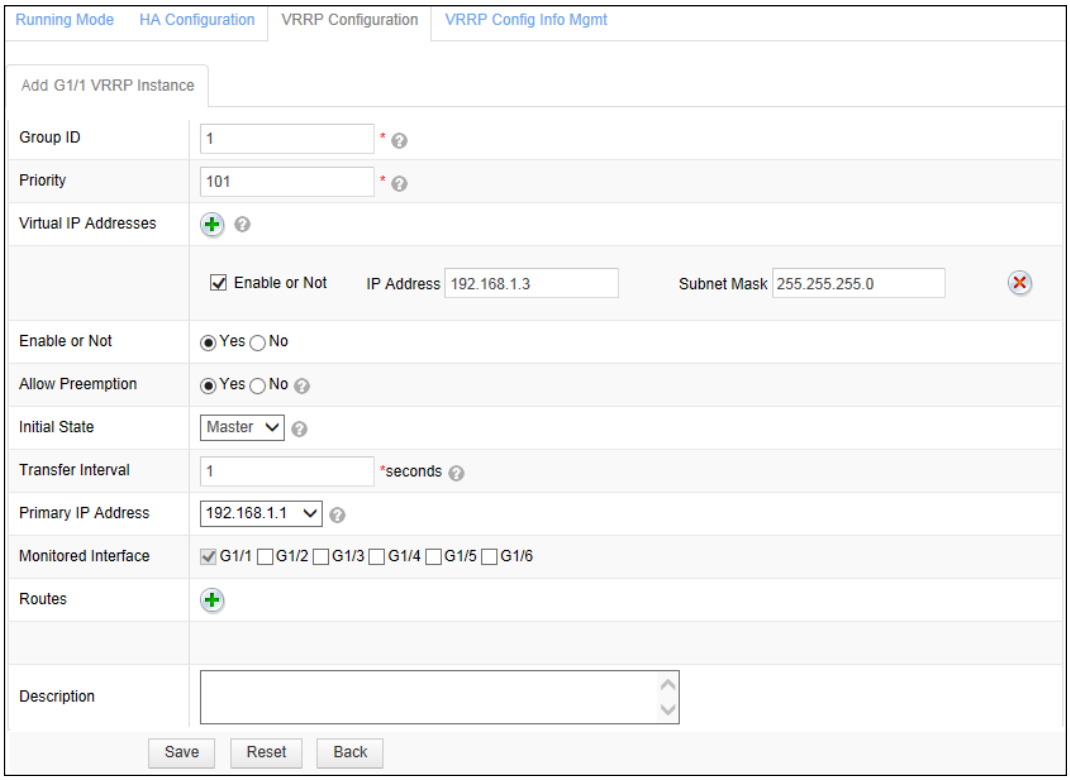
Do as follows to configure VRRP on WAF A as administrator **admin**:

Step 1 Specify a working interface on WAF A.

For details, see steps 1 to 5 in Configuration Procedure on WAF A in section 5.1 Configuring a Single VRRP Group.

Step 2 On the page shown in Figure 5-12, click **Add** to create the first VRRP instance.

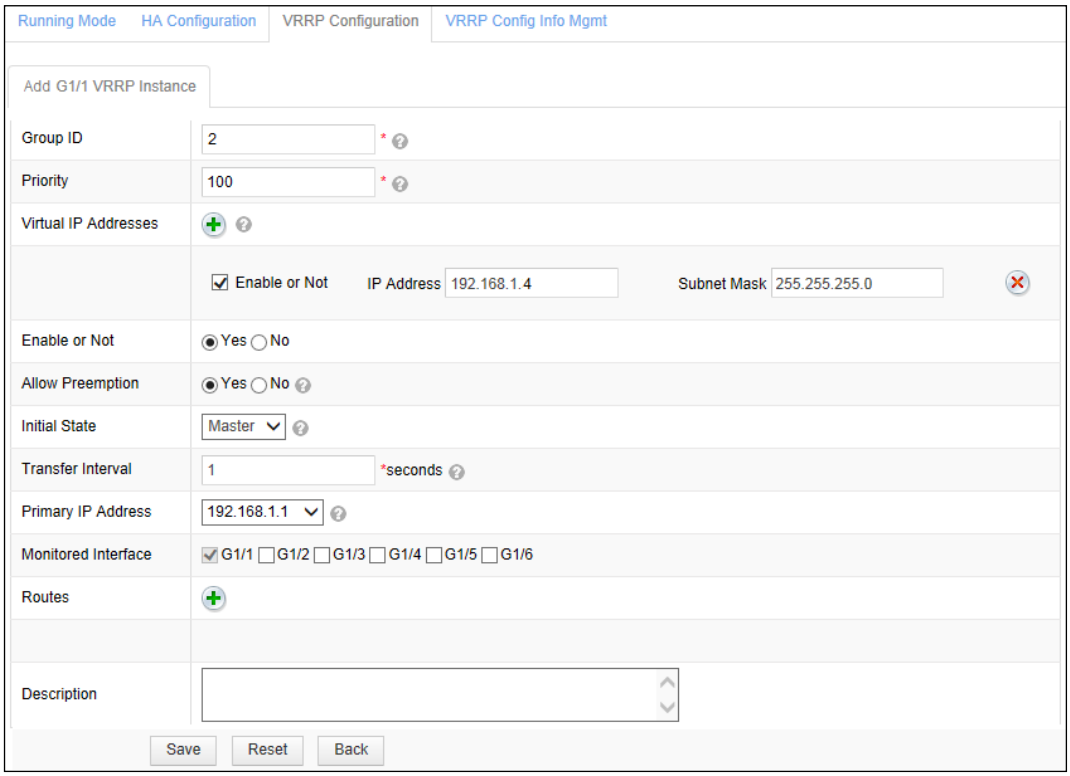
Figure 5-15 Creating the first VRRP instance on WAF A



Step 3 Configure parameters and click **Save** to commit the settings.

Step 4 On the page shown in Figure 5-12, click **Add** to create the second VRRP instance.

Figure 5-16 Creating the second VRRP instance on WAF A



Step 5 Configure parameters and click **Save** to commit the settings.

----End

Configuration Procedure on WAF B

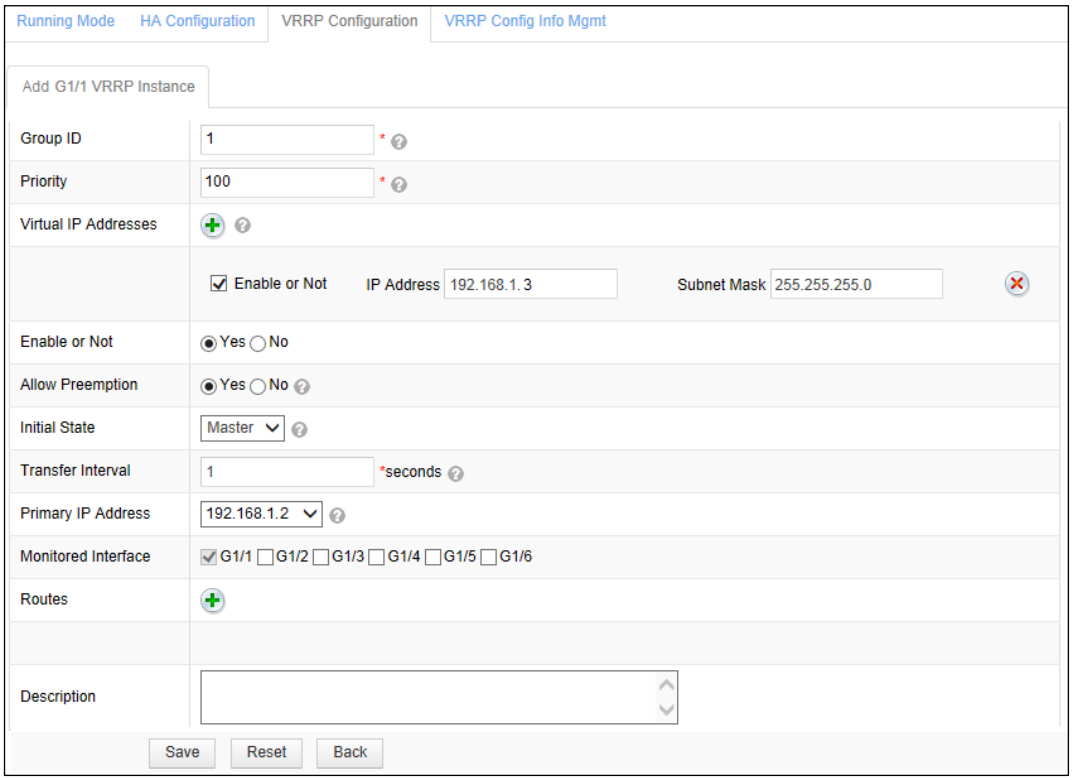
Do as follows to configure VRRP on WAF B as administrator **admin**:

Step 1 Specify a working interface on WAF B.

For details, see steps 1 to 5 in Configuration Procedure on WAF A in section 5.1 Configuring a Single VRRP Group.

Step 2 On the page shown in Figure 5-12, click **Add** to create the first VRRP instance.

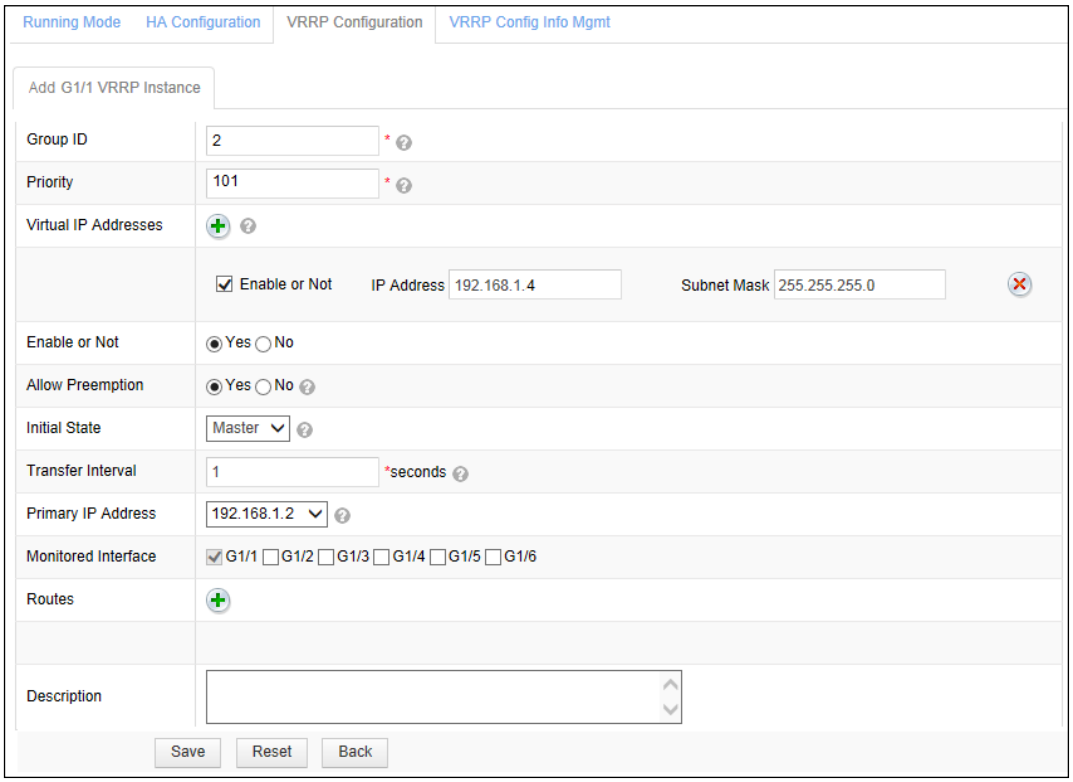
Figure 5-17 Creating the first VRRP instance on WAF B



Step 3 Configure parameters and click **Save** to commit the settings.

Step 4 On the page shown in Figure 5-12, click **Add** to create the second VRRP instance.

Figure 5-18 Creating the second VRRP instance on WAF B



Step 5 Configure parameters and click **Save** to commit the settings.

Note	You must ensure that configuration information of the protected website on WAF A is the same as that on WAF B.

----End

Verification

On the upstream network of WAF, the F5 load balancing device evenly divides traffic destined for the server under WAF's protection and distributes it to the virtual IP addresses 192.168.1.3 and 192.168.1.4. Normally, traffic to 192.168.1.3 is handled by WAF A (master) and traffic to 192.168.1.4 is handled by WAF B (master).

During this process, WAF A and WAF B work simultaneously. In the two VRRP instances configured, the two devices work in master/slave mode to share the load. When one device becomes faulty, the other device takes up all the load, thereby ensuring business continuity.

A Default Parameters

A.1 Default Settings of the Management Interface

IP Address	eth0:192.168.0.1
Subnet Mask	255.255.255.0

A.2 Default Accounts

	User Name	Password
Web Administrator	admin	admin
Web Auditor	auditor	auditor
System Maintainer	maintainer	maintainer
Console Administrator	nsadmin	nsadmin

A.3 Communication Parameters of Console Port

Baud Rate	115200
Data Bit	8
Parity	None
Stop Bit	1
Data Flow Control	None