



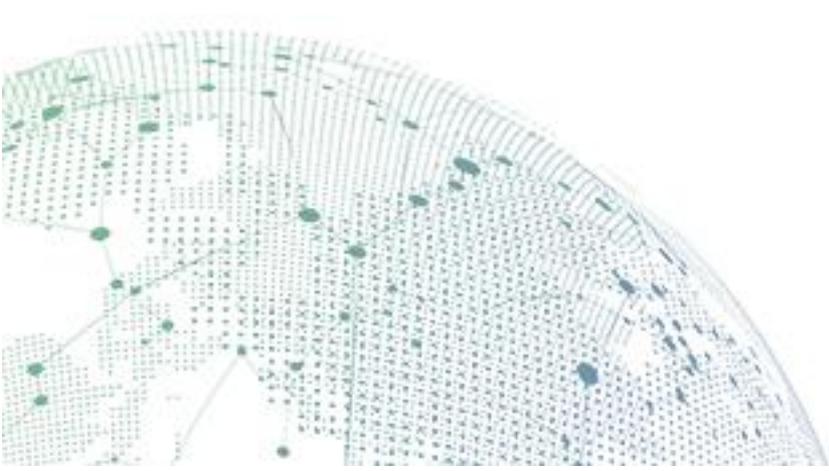
SANGFOR



IAM

Bypass Mode Deployment

Version 12.0.13



Change Log

Date	Change Description

CONTENT

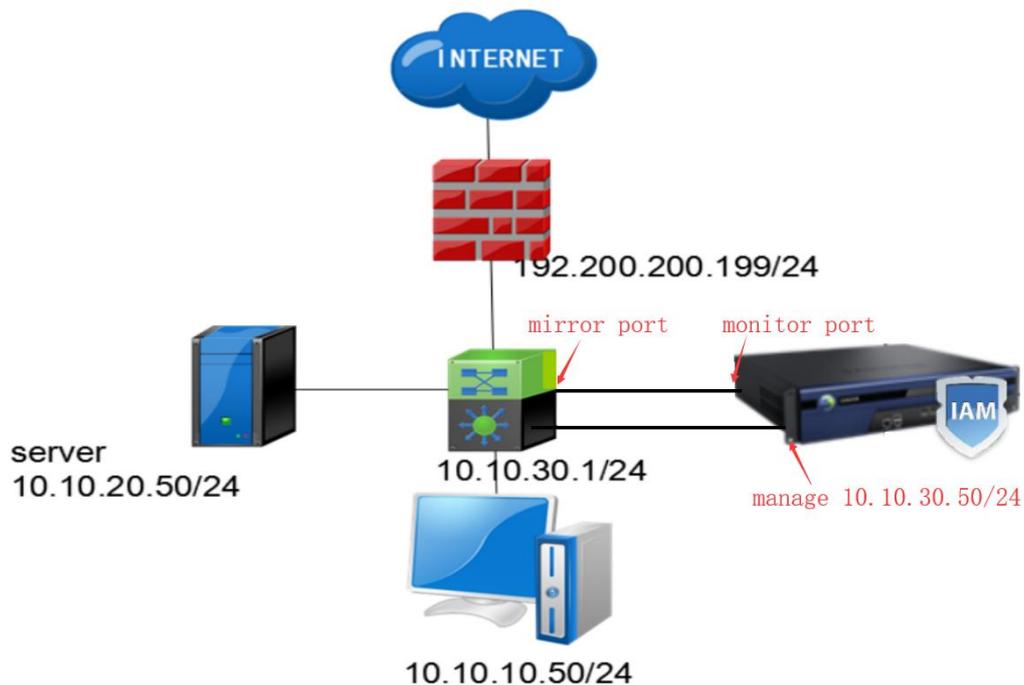
Chapter 1 Applicable Environment	4
Chapter 2 Application Scenario	4
Chapter 3 Configuration Steps	5
5.1 Configuration on IAM.....	5
Chapter 4 Precautions.....	10

Chapter 1 Applicable Environment

1. Bypass mode mainly used for auditing, user has no need to change their network environment. Through connecting the device listening port to the switch mirroring port to achieve the data traffic monitoring.
2. Bypass mode will only useful for auditing base on TCP application control. However, UDP protocol cannot be control. It does not support bandwidth management, NAT, VPN, DHCP features. This deployment mode will not affecting the network environment even when the device is down.

Chapter 2 Application Scenario

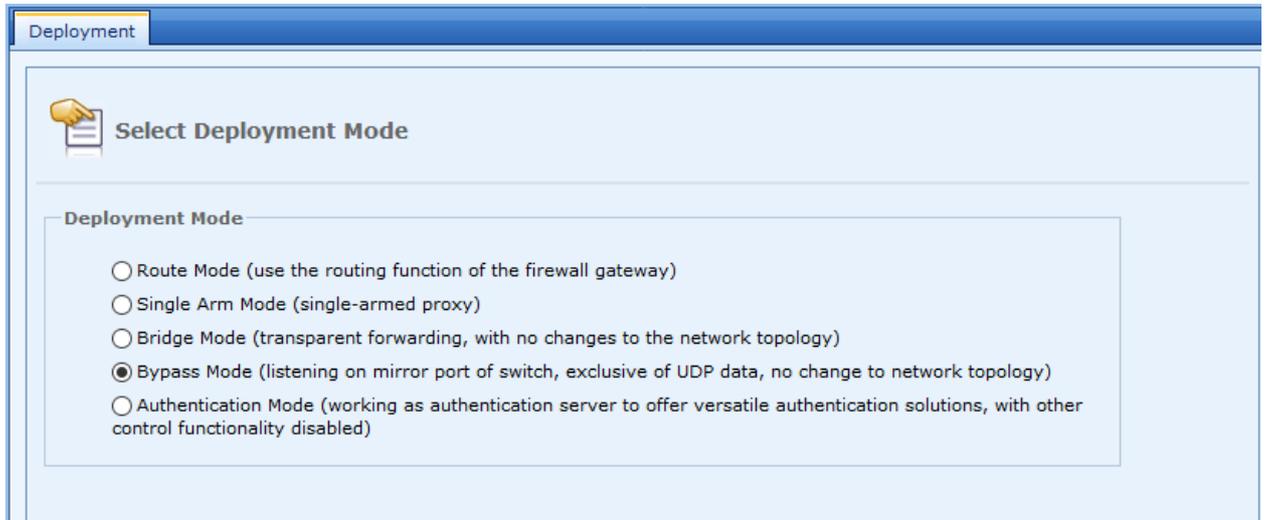
Topology Diagram



Chapter 3 Configuration Steps

5.1 Configuration on IAM

1. Choose "Bypass Mode" when deploy for your IAM device.



2. Management Port configuration, choose management port and assign an IP, default gateway and DNS address for it.

Navigation << Deployment

System

- Network
 - Deployment
 - Interfaces
 - Protocol Extension
 - Optical Bypass
 - High Availability
 - Routing
 - Advanced
- Firewall
- General
- Diagnostics

Bypass Mode

Manage Interface | Listened IP Addresses | Ready to

Manage Interface: eth0

IPv4

IP Address: One entry per row. IP address, subnet and VLAN ID support. Examples: 200.200.20.1/255.255.255.0, 8/200.200.20.5/255.255.255.0

10.10.30.50/255.255.255.0

Default Gateway: 10.10.30.1

Preferred DNS: 8.8.8.8

Alternate DNS: 202.96.134.133

IPv6

[ATTENTION]

It support IPV6 feature, just tick on the IPV6 can do this and user can assign IPV6 form IP in this configuration step.

The screenshot shows a network configuration interface titled "Deployment" with a "Bypass Mode" progress bar. The progress bar has three stages: "Manage Interface" (completed), "Listened IP Addresses" (in progress), and "Ready to" (pending). Below the progress bar, the "Manage Interface" is set to "eth0". There are two sections for IP configuration: IPv4 and IPv6. The IPv4 section is active, with a checked checkbox and a text area containing "10.10.30.50/255.255.255.0". Below it are fields for "Default Gateway" (10.10.30.1), "Preferred DNS" (8.8.8.8), and "Alternate DNS" (202.96.134.133). The IPv6 section is also active, with a checked checkbox and a text area containing "2000:2000::2001/24". Below it are empty fields for "Default Gateway", "Preferred DNS", and "Alternate DNS". A red box highlights the IPv6 checkbox.

Deployment

Bypass Mode

Manage Interface Listened IP Addresses Ready to

Manage Interface: eth0

IPv4

IP Address: One entry per row. IP address, subnet and VLAN ID support. Examples: 200.200.20.1/255.255.255.0, 88/200.200.20.5/255.255.255.0

10.10.30.50/255.255.255.0

Default Gateway: 10.10.30.1

Preferred DNS: 8.8.8.8

Alternate DNS: 202.96.134.133

IPv6

IP Address: One entry per row. IPv6 address and netmask are separated by forward slash(/). VLAN ID support. Examples: 2001:4008::1/64, 88/2001:4008::2/64

2000:2000::2001/24

Default Gateway:

Preferred DNS:

Alternate DNS:

Configure monitoring network segments, differentiate lan-wan direction data: configure listened server as the same section.

The screenshot shows the 'ss Mode' configuration page for 'Listened IP Addresses'. The progress bar is at the 'Listened IP Addresses' step. The 'Mirror Port' dropdown is set to 'eth1,eth2'. Below it, the 'Listened and Excluded IP Addresses' section contains a text area with the following content:

IP Addresses: One IP address or range per row;
Listened subnet examples: 200.200.20.0/255.255.255.0, 2001:4008::/64
Excluded IP address or range begins with hyphen. Excluded IP range examples:
-200.200.20.14-200.200.20.148, -2001:4008::1-2001:4008::ffff; Excluded IP address examples: -200.200.20.58, -2001:4008::1

The text area contains the following IP addresses:

```
10.10.30.0/255.255.255.0  
10.10.10.0/255.255.255.0  
10.10.20.0/255.255.255.0
```

Red annotations include a box around the 'eth1,eth2' dropdown with an arrow pointing to the text: 'Mirroing port cen be one or more than one Depends on their network condition.' Another red box highlights the IP addresses with an arrow pointing to the text: 'Listened Address range is internal network which will be monitored, those are not in the list will be taken as external network, this method to differentiate lan-wan data traffic'.

The screenshot shows the 'Deployment' configuration page for 'Listened Servers'. The progress bar is at the 'Listened Servers' step. The 'Mirror Port' dropdown is set to 'eth1,eth2'. Below it, the 'Listened and Excluded IP Addresses' section contains a text area with the following content:

IP Addresses: One IP address or range per row;
Listened subnet examples: 200.200.20.0/255.255.255.0, 2001:4008::/64
Excluded IP address or range begins with hyphen. Excluded IP range examples:
-200.200.20.14-200.200.20.148, -2001:4008::1-2001:4008::ffff; Excluded IP address examples: -200.200.20.58, -2001:4008::1

The text area contains the following IP addresses:

```
10.10.30.0/255.255.255.0  
10.10.10.0/255.255.255.0  
10.10.20.0/255.255.255.0
```

Below this is the 'Listened Servers' section, which contains a text area with the following content:

Servers: Monitor and audit access to the following servers by any user(from internal or external network).
Examples: IP range, 200.200.20.14-200.200.20.148 and 2001:4008::1-2001:4008::ffff, IP address, 200.200.20.58 and 2001:4008::1"

The text area contains the following IP address:

```
10.10.20.50
```

Red annotations include a box around the 'Listened Servers' section header. Another red box highlights the text: 'Monitor and audit access to the following servers by any user(from internal or external network)'. A third red box highlights the IP address '10.10.20.50'.

Configuration complete, click commit and the device will restart. After this configuration will be valid.

The screenshot displays a network configuration interface with a blue header labeled "Deployment". Below the header, a progress bar shows three steps: "Bypass Mode" (checked), "Manage Interface" (checked), and "Ready to Complete" (checked and highlighted with a red box). The "Ready to Complete" step is the current active step.

Below the progress bar, the configuration details are shown in three sections:

- Manage Interface(eth0)**
 - IP Address: 10.10.30.50/255.255.255.0
 - Default Gateway: 10.10.30.1
 - Preferred DNS: 8.8.8.8
 - Alternate DNS: 202.96.134.133
- Listened and Excluded IP Addresses**
 - 10.10.30.0/255.255.255.0
 - 10.10.10.0/255.255.255.0
 - 10.10.20.0/255.255.255.0
- Listened Servers**
 - 10.10.20.50

At the bottom right of the interface, there are three buttons: "Cancel", "Back", and "Commit". The "Commit" button is highlighted with a red box.

1. Static route configuration, user can assign it during the process of deploying IP for management port and gateway address,
2. New authentication policy, configure the authentication mode based on client's requirement and it almost complete the entire configuration. Ready to host and run.
3. Configure the access control policies based on client's requirements as well.

Chapter 4 Precautions

1. IAM bypass mode deployment will use proxy to surf internet for internal users; it will pass the data traffic in between the internal users and the proxy to the mirroring port of IAM
2. **【Attention on Configuration】** Take note that user needs to eliminate the IP of proxy server from the listening list during configuration.



Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

The information in this document is subject to change without notice.

To obtain the latest version, contact the international service center of SANGFOR Technologies Inc