



SANGFOR



IAM

VLAN Deployment Guide

Version 12.0.18



Change Log

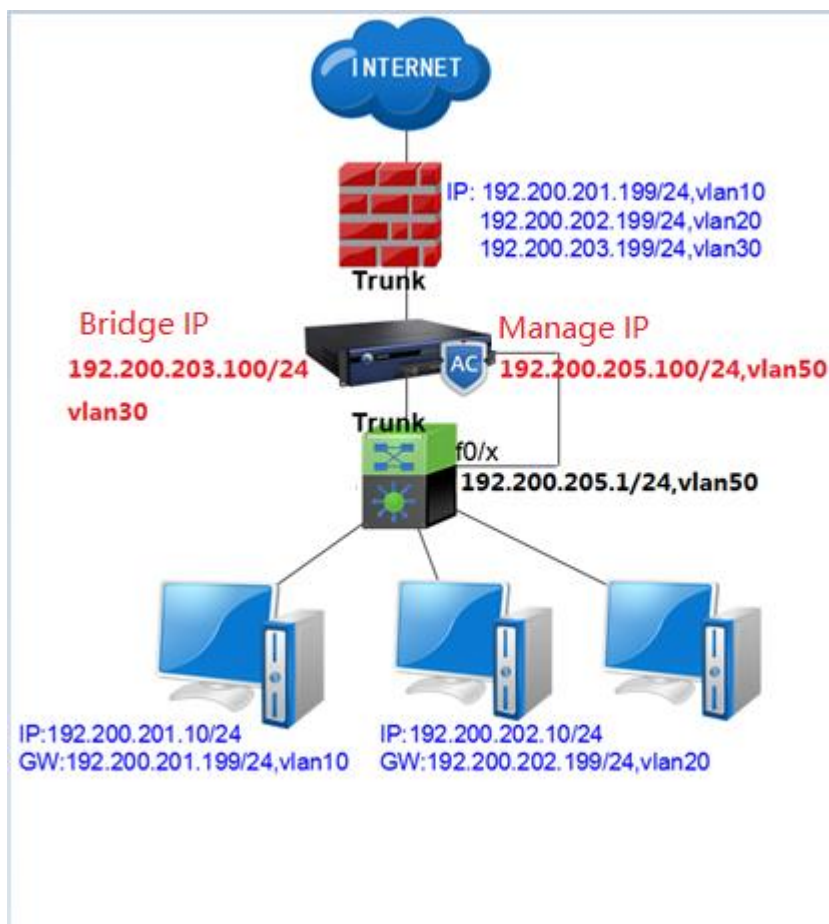
Date	Change Description
July 1, 2019	Version 12.0.18 document release.

CONTENT

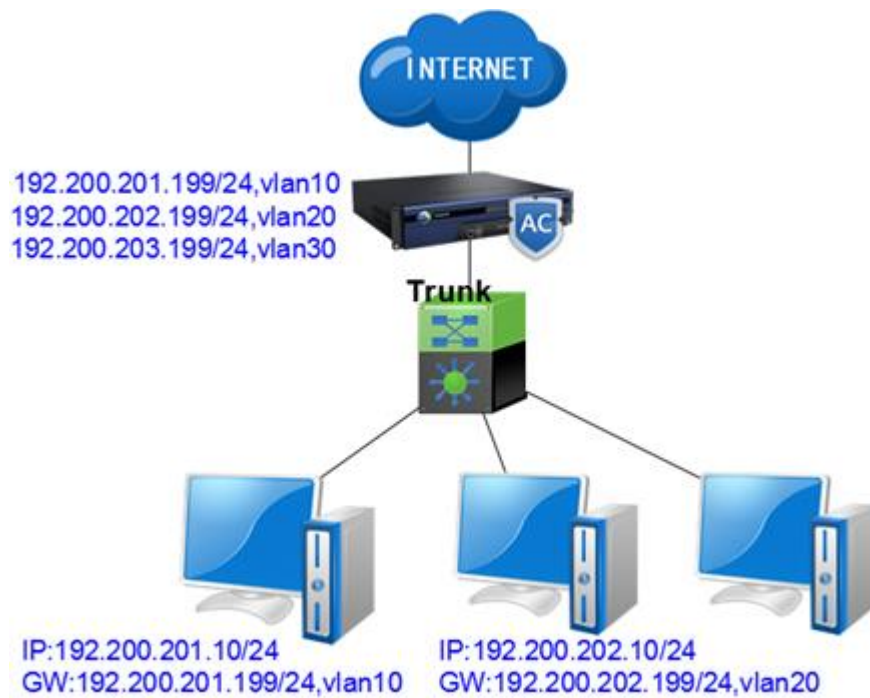
1	Application Scenarios.....	1
2	Configuration Steps	2
2.1	Scenario 1: Bridge mode deployment.....	2
2.2	Scenario 2: Route mode deployment.....	7
3	Precautions.....	14

1 Application Scenarios

Scenario 1: IAM is deployed in bridge mode between the core switch and the front firewall, multiple VLAN data pass through the device. x version bridge mode uses virtual IP for redirection and management of IAM device, at this time there is no need to configure the bridge IP. However, when the IAM device wants to update the database, then need to configure the bridge IP or management address to let IAM access to the Internet.



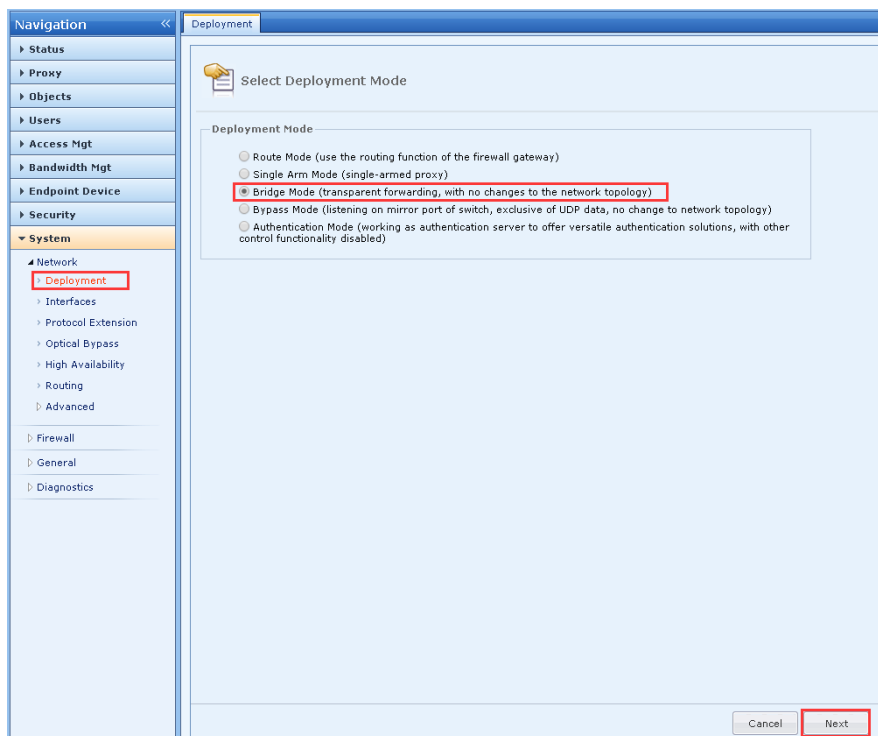
Scenario 2: The IAM is deployed in route mode above the core switch as a network exit. The gateway of each VLAN points to the IAM device.



2 Configuration Steps

2.1 Scenario 1: Bridge mode deployment

1. Configure the deployment mode as bridge mode.



2. Select the interface list.

Bridge Mode

Progress bar: Interfaces (selected), Bridge Interfaces, Manage Interface, Gateway, Ready to Complete

Bypass Interface Pair: eth0<->eth2

Interface

Available LAN Interface

- eth1(GE)
- eth3(GE)

Available WAN Interface

- eth1(GE)
- eth3(GE)

Bridge (LAN<->WAN)

- eth0(GE)<->eth2(GE)

Add **Delete**

☐ **Enable bridge state propagation** (if one tracked bridge changes status between Connected and Disconnected, the other bridge changes accordingly, telling the peer device that the local device is down or recovers in redundant network)

Interfaces Tracking:
eth0<->eth2 supports link state propagation

Cancel **Back** **Next**

3. Configure the bridge IP address. (optional step, if you use the management port to manage the device, you no need to configure the bridge address)

The screenshot shows a configuration window titled "Bridge Mode" with a progress bar at the top. The progress bar has five steps: "Interfaces" (checked), "Bridge Interfaces" (active), "Manage Interface", "Gateway", and "Ready to Complete". Below the progress bar, the "Bridge1(eth0<->eth2)" tab is selected. Under this tab, the "IPv4" checkbox is checked and highlighted with a red box. Below it, the "IP Address:" label is followed by a text area containing the example "30/192.200.203.100/255.255.255.0", which is also highlighted with a red box. The "IPv6" checkbox is unchecked. At the bottom right, there are three buttons: "Cancel", "Back", and "Next", with the "Next" button highlighted by a red box.

Bridge Mode

Interfaces Bridge Interfaces Manage Interface Gateway Ready to Complete

Bridge1(eth0<->eth2)

☒ 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
30/192.200.203.100/255.255.255.0

☐ IPv6

Cancel Back Next

4. Configure the management port. (optional step, if the bridge IP is configured to manage the device, you no need to configure the management port)

Bridge Mode

Interfaces Bridge Interfaces Manage Interface Gateway Ready to Complete

Manage Interface: eth1

☒ IP v4

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

10.252.252.252/255.255.255.0
50/192.200.205.100/255.255.255.0

☐ IP v6

Cancel Back Next

5. Configure the gateway and DNS, used for the device to online update the database.

Note: If you use a bridge to manage the device, the default gateway is the gateway address of the bridge address (that is, 192.200.203.199); if you use the management port to manage the device, the default gateway is the gateway of the management port (that is, 192.200.205.1).

Bridge Mode

Progress: Interfaces ☒ Bridge Interfaces ☒ Manage Interface ☒ Gateway ☐ Ready to Complete ☐

☒ **IPv4**
Default Gateway:
Preferred DNS:
Alternate DNS:

☐ **IPv6**

☒ **Bypass firewall rule** (recommended, this allows data flow between WAN and LAN interfaces)

Cancel Back **Next**

6. Applying the configuration will prompt you to restart the device.

Bridge Mode

☒ Interfaces
 ☒ Bridge Interfaces
 ☒ Manage Interface
 ☒ Gateway
 ☒ Ready to Complete

MANAGE Interface (eth1): 10.252.252.252/255.255.255.0
50/192.200.205.100/255.255.255.0

Bypass firewall rule: Enable

Default Gateway: 192.200.203.199

Preferred DNS: 180.76.76.76


Alternate DNS: 114.114.114.114

Bridge1(eth0<->eth2)

Bridge Interface 30/192.200.203.100/255.255.255.0

Bridge: eth0<->eth2

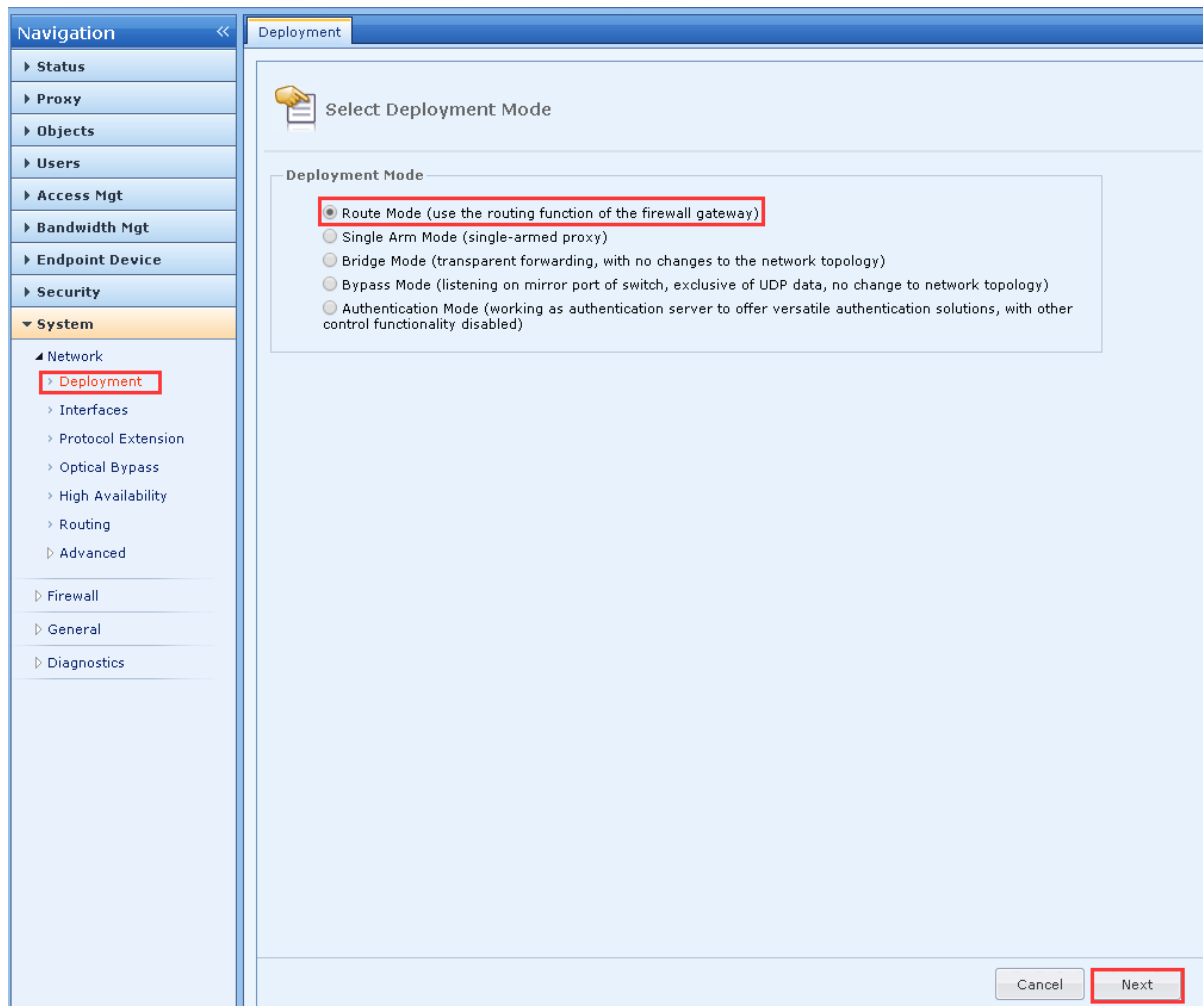
Deployment


 The device is required to restart if you save changes to deployment mode. Are you sure to continue and log in again later?

7. Create a new authentication policy, set the corresponding authentication policy according to customer requirements, and the device can be put on use.

2.2 Scenario 2: Route mode deployment

1. Configure the deployment mode as route mode.



2. Select the interface list.

Route Mode

Progress: Interfaces (selected) | LAN Interface | WAN Interface | DMZ Interface | NAT | Ready to Complete

Interface

Available Interface

eth3(GE)

Add ▶

Delete ◀

LAN Interface

eth0(GE)

Add ▶

Delete ◀

WAN Interface

eth2(GE)

Add ▶

Delete ◀

DMZ Interface ⓘ

eth1(GE)

Add ▶

Delete ◀

Cancel Back **Next**

3. Configure the LAN port.

Route Mode

Interfaces LAN Interface WAN Interface DMZ Interface NAT Ready to Complete

eth0

☒ IPv4

IP Address: One entry per row. Separate IP address and mask with forward slash(/). VLAN ID support. Examples: 200.200.20.1/255.255.255.0, 200.200.20.1-200.200.20.5/255.255.255.0, 88/200.200.20.5/255.255.255.0. If VLAN ID is changed, the DHCP server must be changed accordingly.

10/192.200.201.199/255.255.255.0
20/192.200.202.199/255.255.255.0
30/192.200.203.199/255.255.255.0

☐ IPv6

Cancel Back Next

4. Configure the WAN port and configure the gateway and DNS.

Route Mode

Interfaces LAN Interface WAN Interface DMZ Interface NAT Ready to Complete

eth2

Address: Specified

☒ IPv4

IP Address: One entry per row. Subnet and IP range support. Examples:
200.200.20.1/255.255.255.0 200.200.20.1-200.200.20.5/255.255.255.0
10.1.2.16/255.255.255.0

Default Gateway: 10.1.2.1

Preferred DNS: 180.76.76.76

Alternate DNS: 114.114.114.114

☐ IPv6

Cancel Back Next

5. Configure the DMZ port.

Route Mode

Interfaces LAN Interface WAN Interface DMZ Interface NAT Ready to Complete

eth1

☒ IPv4

IP Address: One entry per row. Separate IP address and mask with forward slash(/). VLAN ID support. Examples: 200.200.20.1/255.255.255.0, 200.200.20.1-200.200.20.5/255.255.255.0, 88/200.200.20.5/255.255.255.0. If VLAN ID is changed, the DHCP server must be changed accordingly.

10.252.252.252/255.255.255.0

☐ IPv6

Cancel Back Next

6. Configure the NAT to access the Internet.

Route Mode

Interfaces LAN Interface WAN Interface DMZ Interface NAT Ready to Complete

Name: Source NAT

WAN Interface: Any WAN interface

Source Address: One entry per row. IPv4 address and netmask are separated by forward slash(/). Example: 192.168.0.1/255.255.255.0

192.200.201.0/255.255.255.0
192.200.202.0/255.255.255.0
192.200.203.0/255.255.255.0

Map Src IP To: WAN interface IP

[DNS Service](#)

[ALG NAT and ESP](#)

Cancel Back Next

7. Applying the configuration will prompt you to restart the device

Route Mode

Interfaces LAN Interface WAN Interface DMZ Interface NAT Ready to Complete

LAN Interface

eth0

IP Address: 10/192.200.201.199/255.255.255.0
20/192.200.202.199/255.255.255.0
30/192.200.203.199/255.255.255.0

WAN Interface

eth2

Line Type: Ethernet
IP Address: 10.1.2.16/255.255.255.0
Default Gateway: 10.1.2.1
Preferred DNS: 180.76.76.76
Alternate DNS: 114.114.114.114

DMZ Interface

eth1

IP Address: 10.252.252.252/255.255.255.0

NAT

Name: Source NAT
WAN Interface: Any WAN interface
Source Address: 192.200.201.0/255.255.255.0
192.200.202.0/255.255.255.0
192.200.203.0/255.255.255.0
Mapped Src IP: WAN interface IP

Cancel Back **Commit**

Deployment

The device is required to restart if you save changes to deployment mode. Are you sure to continue and log in again later?

Yes No

8. Create a new authentication policy, set the corresponding authentication policy according to customer requirements, and the device can be put on use.

3 Precautions

1. After the device sets the default gateway, it will generate a default route, which does not need to be added again.
2. When the device is deployed in bridge mode, the internal network can manage the device through the virtual IP address. The default virtual IP address is 1.1.1.3, access through https://1.1.1.3, and the device can be logged in. It is not recommended to modify the address. Please consult the technical support first if want to modify the address.

The screenshot displays the Sangfor IAM configuration interface. On the left, the 'Navigation' pane shows a tree structure with 'System' expanded and 'Advanced' selected. The 'Category' pane on the right lists various settings, with 'Redirection/Proxy' highlighted. The main configuration area, titled 'Redirection/Proxy', contains three sections: 'Redirection', 'Proxy', and 'Virtual IP'. The 'Redirection' section has two checkboxes, both of which are unchecked. The 'Proxy' section also has two checkboxes, both unchecked. The 'Virtual IP' section contains two input fields: 'IPv4 Address' with the value '1.1.1.3' and 'IPv6 Address' with the value '1::3'. A 'Commit' button is located at the bottom right of the configuration area.

Navigation << Advanced

Category << Redirection/Proxy

Redirection ⓘ

☐ Enable destination based routing, and specify port to forward redirected data

☐ DMZ Port Redirection ⓘ

Proxy ⓘ

☐ Enable destination based routing, and specify port to forward proxy data

☐ Do not restore address ⓘ

Virtual IP

IPv4 Address: 1.1.1.3

IPv6 Address: 1::3

Commit



SANGFOR

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