SANGFOR

IAM

Vmware for vIAM Implementation Guide

Version 11.x and above

Change Log

Date	Change Description
November 13, 2020	Version 11.x and above document release.

CONTENT

Chapter 1 Introduction

Sangfor IAM, hereinafter referred to as vIAM, support to be deployed in the virtual environment of VMware. vIAM provides an ova template that can be deployed in Vmware and for authorized use.

Chapter 2 Implementation

1. Download vIAM template:
   https://download.sangfor.com/Download/Product/IAM/VM/IAM11.9_20170620.ova

2. Import the virtual machine template into the virtualization platform, where you can import vIAM as a normal Linux server. Specifically, follow the platform's virtual machine import instructions to import it.

   Note: The current provided vIAM virtual machine template supports VMware ESXi 5.0 and above.

3. Edit virtual machine configuration. The default hardware configuration of the virtual machine template provided is as follows:

   CPU: 4
   Memory: 8G
   Number of network ports: 6
   Disk size: 80G

   Among them, the CPU and memory can be adjusted as needed. Network ports can also be added as needed, and at least 3 network ports are required to work properly. The disk size does not support adjustment. If you need a larger virtual disk, you need to download the corresponding template.

   Below is the authorized bandwidth and vIAM recommended configuration reference table, maximum support 2G bandwidth:

V Type	Performance	Recommended CPU	Recommended Memory
vAC-50	50M	1vCPU	2G
vAC-100	100M	1vCPU	2G
vAC-200	200M	2vCPU	4G
vAC-300	300M	4vCPU	8G
vAC-500	500M	4vCPU	8G
vAC-700	700M	4vCPU	8G
vAC-1000	1G	8vCPU	16G
vAC-2000	2G	8vCPU	16G

4. Modify the vIAM management address.

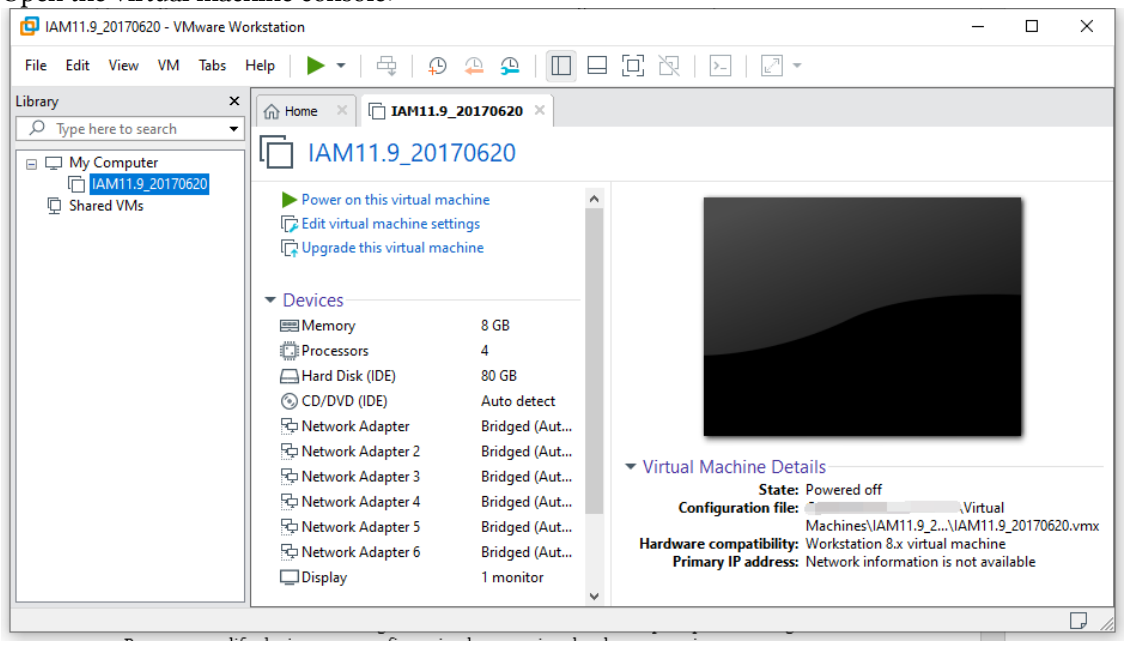
   Modify the configuration of the vIAM virtual machine and connect the DMZ port (eth1) of the device to a PC's virtual network interface that can communicate with the vIAM, and connect the WAN port (eth2) of the device to a virtual network that can access the external network. After the vIAM is turned on, it must first obtain or configure the DMZ port IP, which is used to access the

management console page.

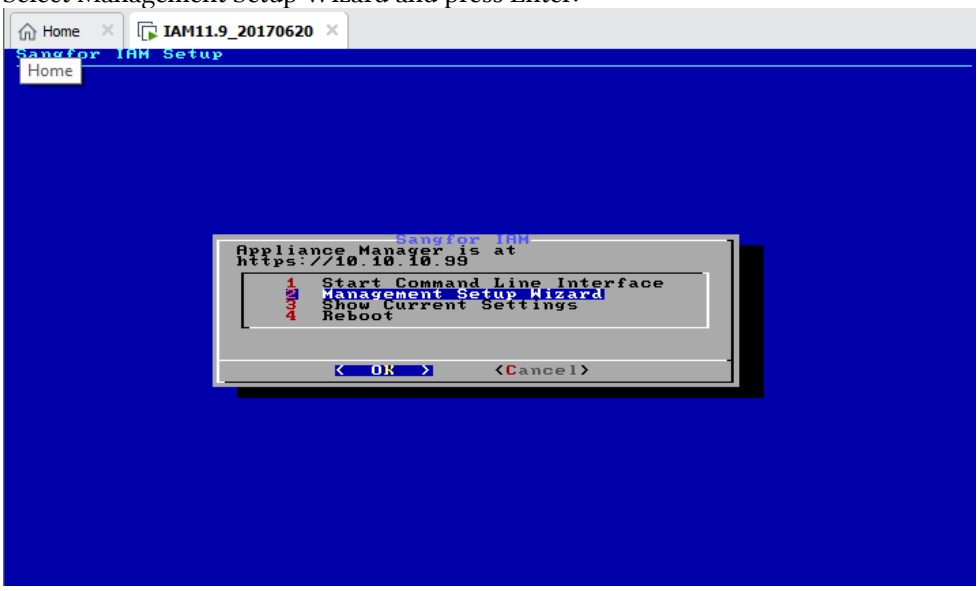
There are two ways to access the IP address of the DMZ port of the device:
(1) Configure the PC with the IP address of the same network segment and directly connect to the default IP address of the DMZ port: 10.252.252.252/24 or 128.128.125.252/28, but it is necessary to ensure that there is no IP conflict in the network.
(2) Open the Vmware console and modify the IP address of the DMZ port.

The first method will not be explained here. The second way, configure the DMZ port IP address of vIAM through the Vmware console is shown as below, which can be used as a reference for configuration of other platforms:

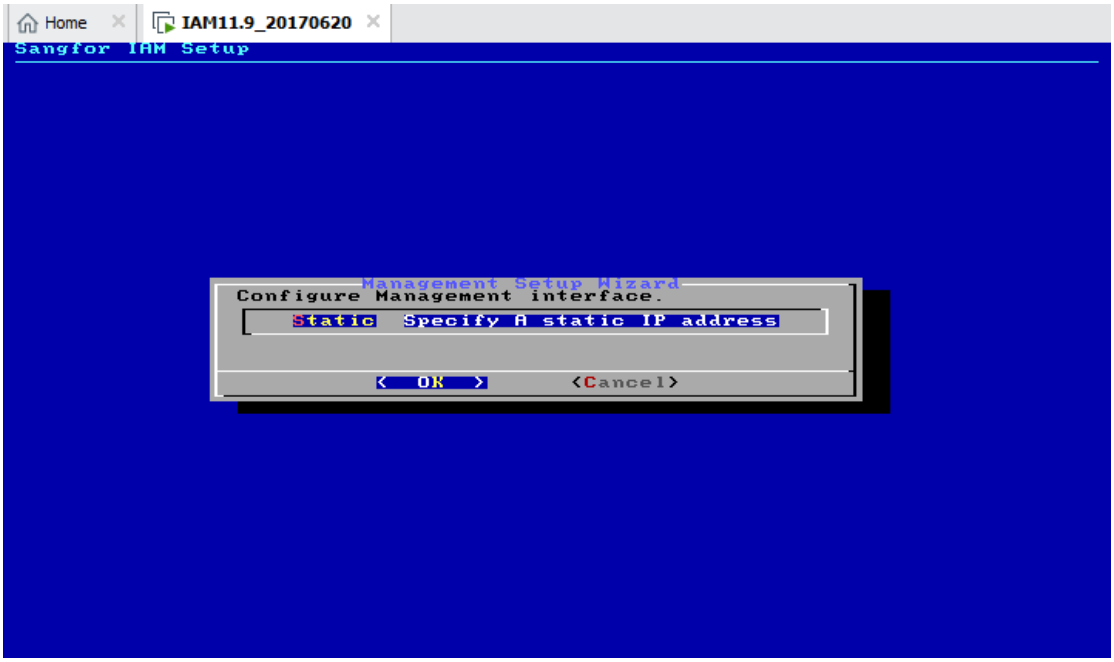
(1) Open the virtual machine console:



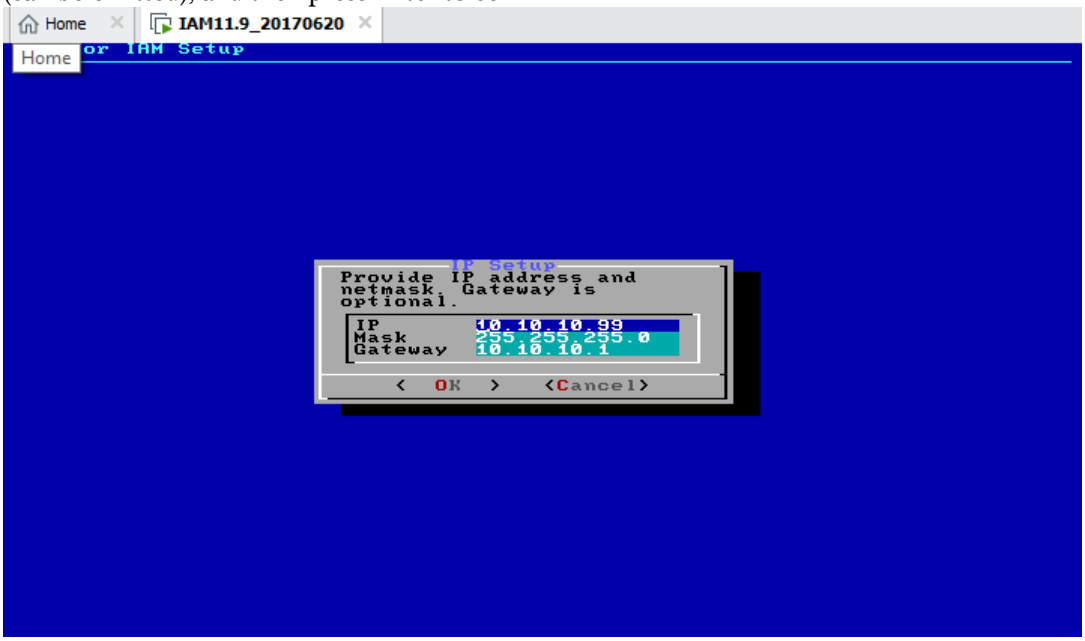
(2) Select Management Setup Wizard and press Enter:



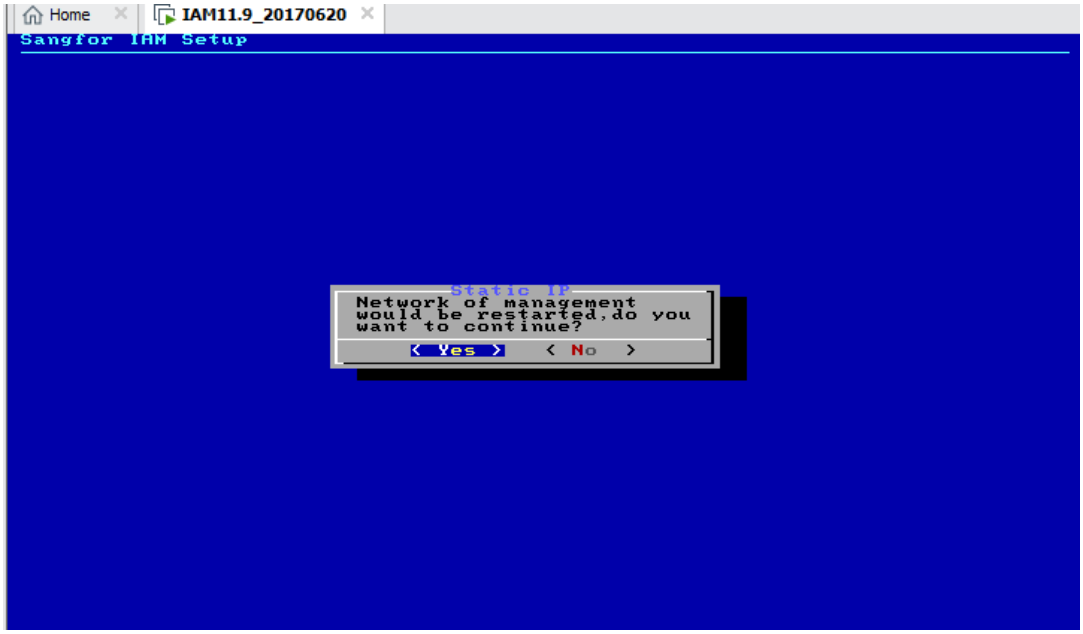
(3) Select OK:



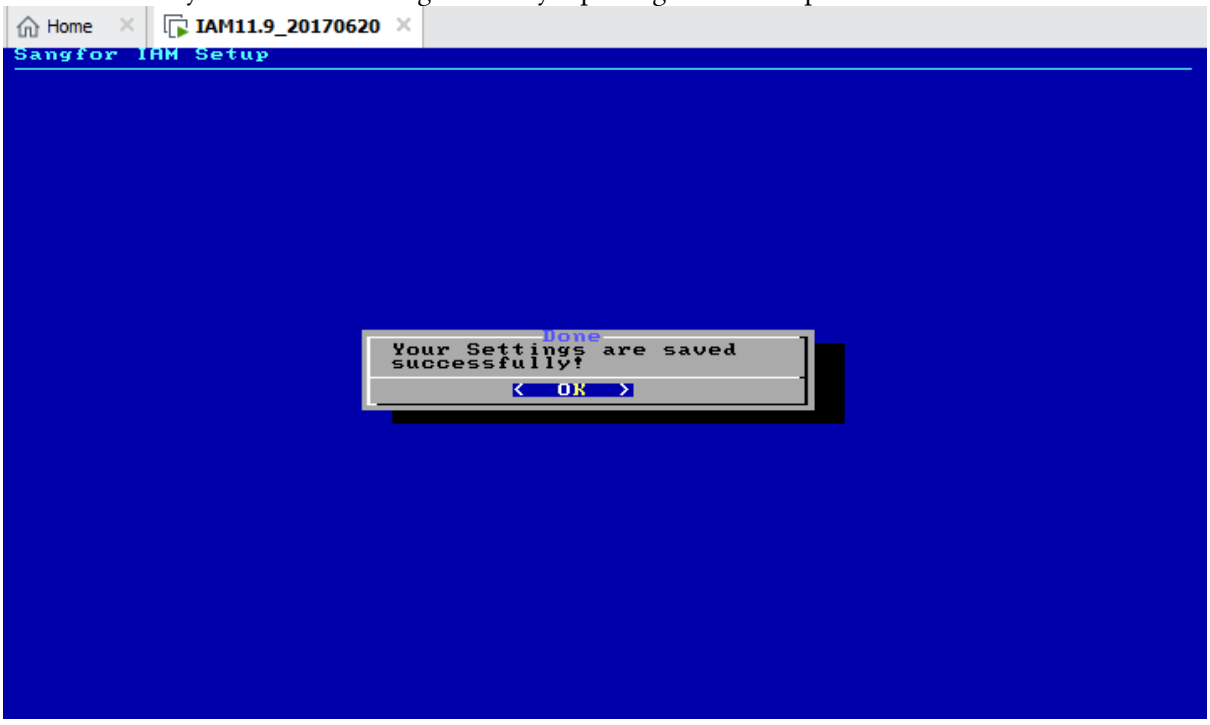
(4) The IP configuration page appears, fill in the IP address, mask and gateway to be configured (can be omitted), and then press Enter to confirm:



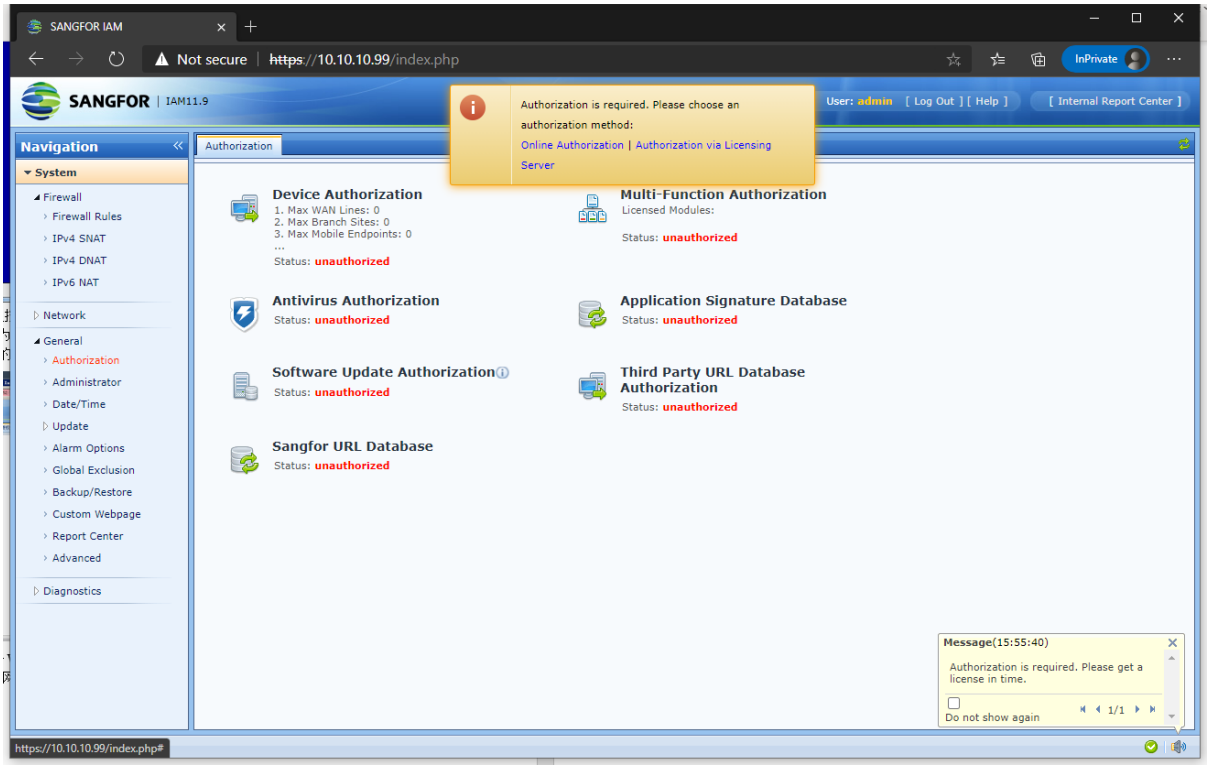
(5) Select Yes:



(6) After a while, the following page will prompt up to indicate that the IP configuration is successful. If the IP or mask configuration is incorrect, there will be a prompt to reconfigure. Return to modify the incorrect configuration by repeating the above operation:

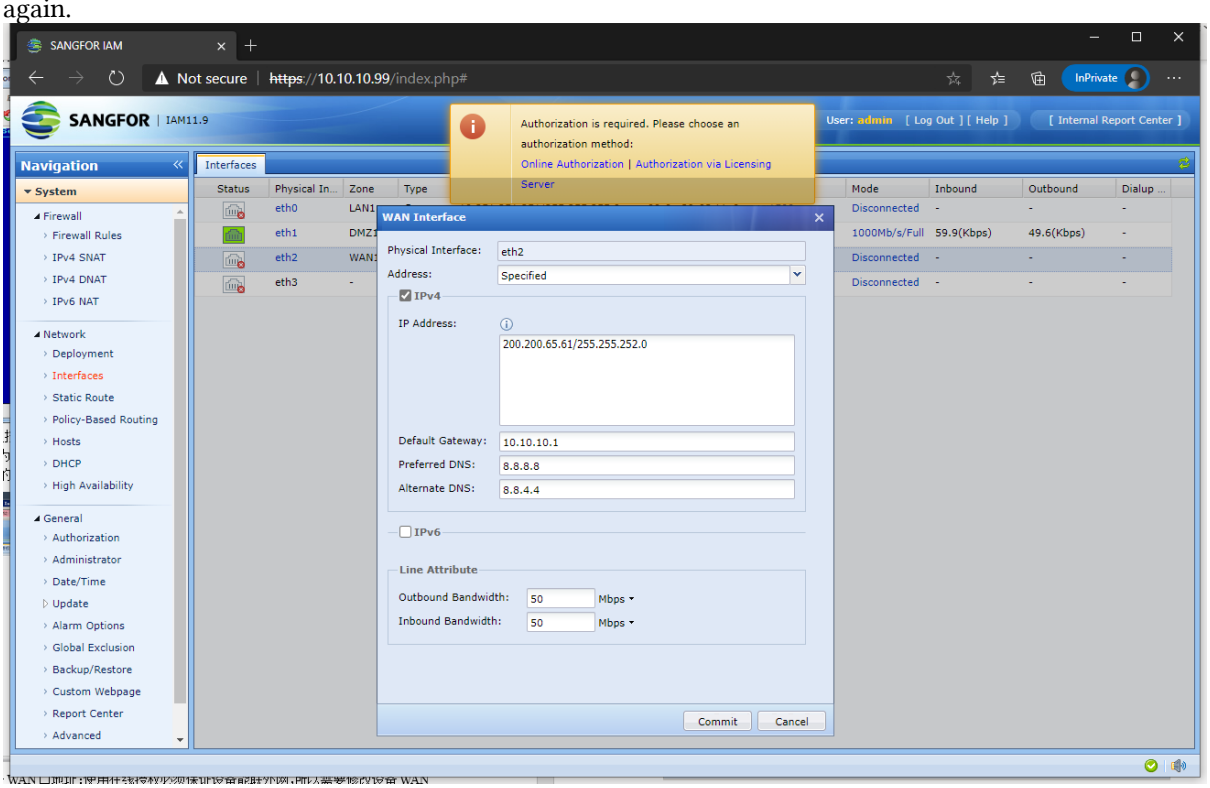


(7) Log in to the management console. After the IP configuration is successful, visit https://[DMZ IP] and log in to the console management interface. The default username and password are admin/admin. Unauthorized devices can only display the system section interface. After the authorization is successful, you can see all the management interfaces after logging in to the device.

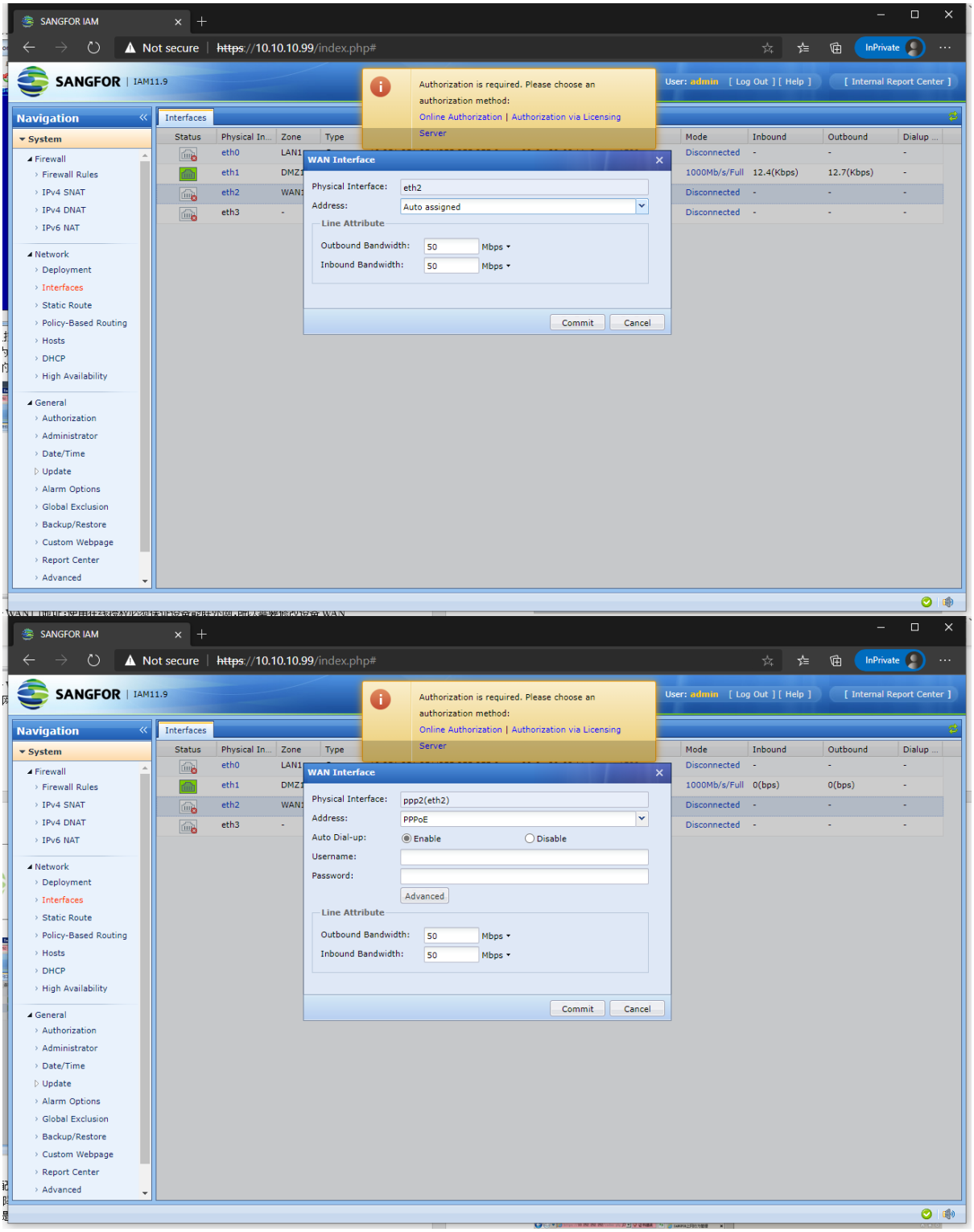


(8) Configure the device's WAN port address. To use online authorization, the device must be able to connect to the external network, so you need to modify the device's WAN port IP address, gateway, and DNS configuration to ensure that the device can access the online authorization server.

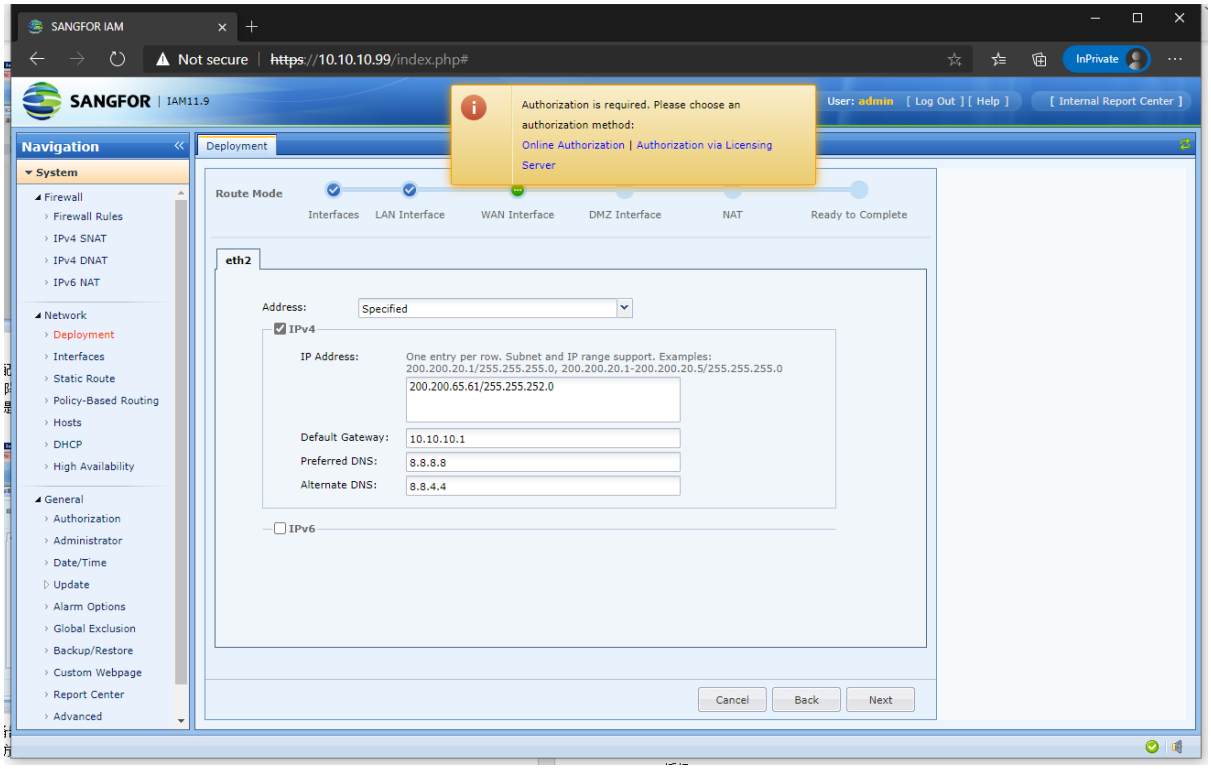
Navigate to System > Network > Interface, open the network port configuration page, and then click WAN (eth2) port, configure IP, mask, default gateway and DNS, and then submit. After submitting the modification, it will automatically log out and you need to log in to the device again.



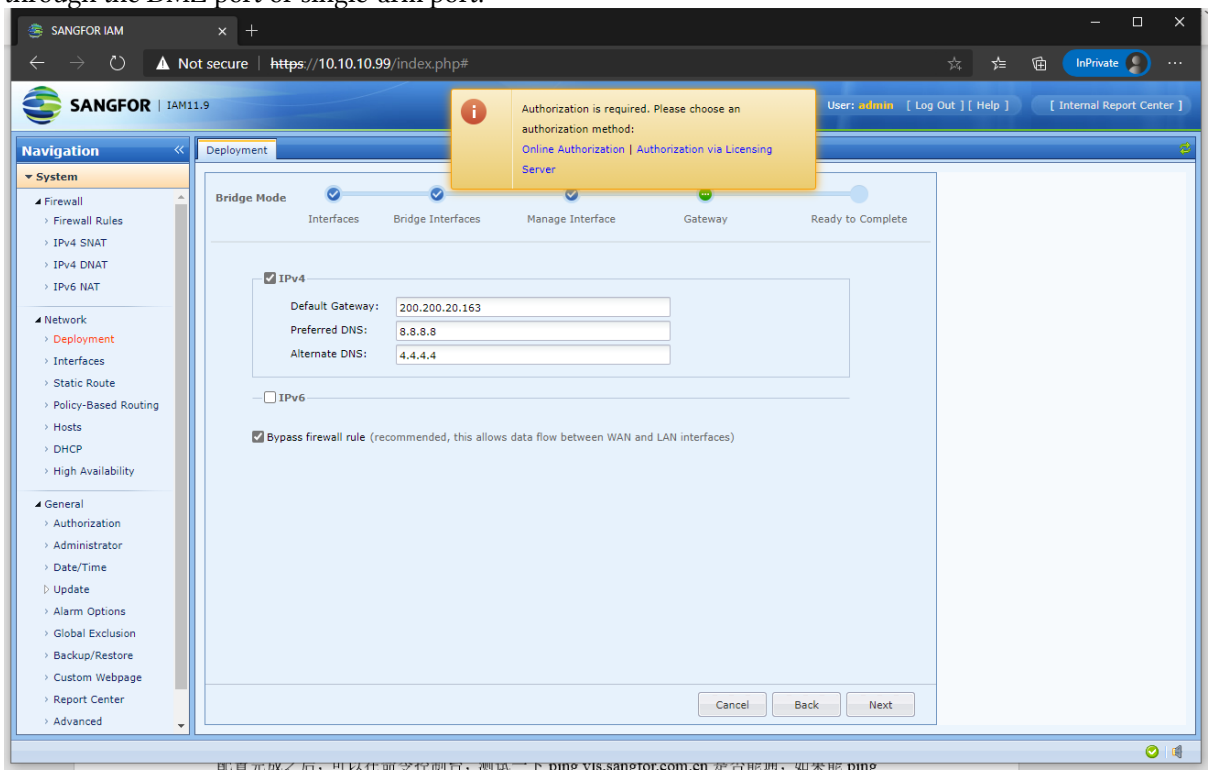
You can also use DHCP or PPPOE dial-up to automatically obtain the WAN port configuration:



In addition to modifying the network port configuration, you can also modify the deployment mode to configure the WAN port address. Click: System > Network > Deployment, open the deployment mode configuration page, and then follow the configuration to configure it step by step, and submit it after the configuration is complete. After submitting the modification, you will be prompted to restart the device, and log in again after the restart is complete:



Note: If the device deployment mode needs to be changed from route mode to bridge mode, bypass mode or single-arm mode, it needs to be configured to access the external network through the DMZ port or single-arm port.



After the configuration is complete, you can test whether ping vls.sangfor.com.cn can work in the command console. If it can ping, the network is available. If the ping fails, you need to confirm whether the default gateway, DNZ or IP address is configured correctly.

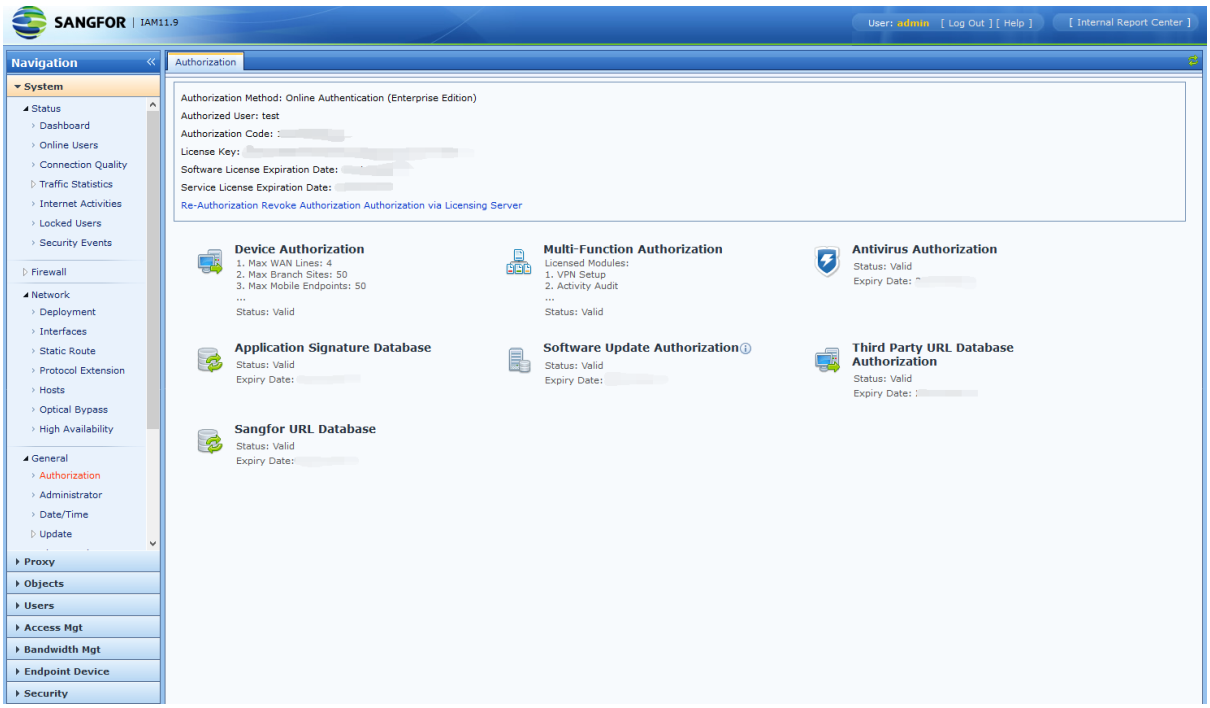
Online authorization:

You can contact local sales for consultation and purchase online authorization. Authorization includes authorization ID and serial number. For example:
Authorization ID: S8234-5678-90AB-CDEF-1234-5678-90AB-CDEF
Serial number: 1234-5678-90AB-CDEF-1234-5678-90AB-CDEF

Click the online authorization link at the top of the console page, then enter the authorization ID and serial number to submit:

After the authorization is successful, the page will prompt to log in again:

After authorization, if it is authorized by bandwidth, the login interface will display the authorized model:



On the authorization page, you can view the current authorization information, authorization time, enabled functions, service hours, etc. Online authorization can change the serial number or delete the authorization.

Note:
To use online authorization, you must ensure that vIAM can remain connected to the Internet. If you cannot connect to the Internet for 7 consecutive days, the authorization will become illegal, the system function will be limited, and the core configuration interface will be hidden and cannot be edited. If you cannot connect to the Internet for 30 consecutive days, the authorization will become invalid, and the business will be interrupted, which may cause the network to be disconnected.

The authorization ID and serial number of online authorization can only be used in one system. If the authorization ID and serial number have been used elsewhere, the authorization ID and

serial number in the original system must be deleted before they can be used on the new system.

Chapter 3 Unsupported Function

1. The crossover cable method is not supported to restore the default configuration, but you can use an alternative solution, enter the vIAM virtual console, and use the command reset_cfg to restore the default configuration.

2. The crossover cable method is not supported to recover the admin password, but you can use an alternative solution, enter the vIAM virtual console and use the command reset_pwd to recover the admin password.

3. Bypass is not supported, including optical bypass and electrical bypass.

4. Does not support GCS activation.

5. Does not support wireless functions.

6. User restrictions on low-end devices are not supported, the authorized bandwidth indirectly limits the number of users.

7. vIAM on VMware platform does not support dual-machine deployment when using online authorization.

Chapter 4 Precautions

1. To use online authorization, you must ensure that vIAM can remain connected to the Internet. If you cannot connect to the Internet for 7 consecutive days, the authorization will become illegal, the system function will be limited, the core configuration interface will be hidden and editing is not allowed, but the business will not be interrupted. If cannot connect to the Internet for 30 consecutive days, the authorization will be invalidated and become an unauthorized state, and the business will be interrupted, which may result in disconnection.

2. The authorization ID and serial number of online authorizations can only be used in one system. If the authorization ID and serial number have been used elsewhere, the authorization ID and serial number in the original system must be deleted before they can be used in the new system.

3. When the authorization is replaced, the flow control of line bandwidth will be automatically reset. If multiple flow control lines are configured, the bandwidth will be divided equally by the line, and the line bandwidth needs to be reconfigured.

4. It is not recommended to deploy vIAM by cloning.

5. When using online authorization, if vIAM is shut down or disconnected for more than 30 days, the authorization will become invalid and you need to re-enter the authorization serial number.

6. The disk size of vIAM does not support adjustment, and additional disks cannot be used. If you need a larger virtual disk, you need to download the corresponding template.

Chapter 5 Common Problems and Troubleshooting Methods

1. The online authorization fails:

   Follow the steps below to troubleshoot step by step:

   a. Open the command console, the location of the command console is: System > Diagnosis > Web Console.

   b. Ping the gateway on the command console to see if it works. If it doesn't, the gateway cannot be accessed. You need to confirm whether the gateway IP is correct and the gateway is available.

   c. Ping the DNS server on the command console. If it fails, the DNS server is unavailable. You need to confirm whether the DNS server IP is correct or change the DNS server.

   d. Ping vls.sangfor.com.cn on the command console. If it fails, it means that the authorized server has abnormal access or limited access. You need to check whether the current access is blocked by the internal network denial policy or perform ping on the PC.

   e. Execute telnet vls.sangfor.com.cn 443 in the command console. If it fails, it means that the authorized server has abnormal access or limited access. It is necessary to determine whether the current access is blocked by the internal network denial policy or execute it on the PC telnet to see if it works.

2. After login to the web console, the system only displays the system configuration page, the other pages are gone:

   a. The possible reason is that the device authorization is illegal, the authorization has expired, the authorization becomes unauthorized, and the authorization is disabled. There will be a prompt at the top of the web console page.

   b. For illegal device authorization caused by long-term failure to connect to the Internet, the authorization status can be restored after the network connection is restored, otherwise the authorization will become invalid after 30 days and the business will be interrupted.

   c. If the authorization has expired, you need to purchase the authorization again, otherwise the authorization will become invalid after 30 days and the business will be interrupted.

   d. For the case where the authorization is disabled, it means that the authorization server has detected that the authorization has been used illegally or the serial number has been disabled.

3. A virtual network port is added but the network configuration page does not display:

   a. Reconfigure the deployment mode and you can see the newly added network port.

4. The console is configured with the DMZ port IP address, but it cannot be connected:

    a. In the console menu page, if the configuration does not take effect or there is a problem with the configuration, please try to reconfigure the DMZ port IP address and default gateway.