

知 ※Experience cases of handling the problem that portal authentication does not take effect in a local forwarding network at a site

Wireless 周天 2020-12-28 Published

Network Topology

Comware V7 platform wireless controller, wireless local forwarding enables portal authentication

Problem Description

After the wireless terminal is associated with the wireless, the portal authentication is not redirected when opening the webpage, but can go online directly, and the portal authentication does not take effect.

Process Analysis

After the wireless terminal is associated with wireless, it will not be redirected for portal authentication when opening the webpage, but can go online directly, and the portal authentication does not take effect.

1. Check the configuration, check whether the related portal configuration is normal, try to send the same portal configuration to the centralized forwarding service template, and the portal functions normally. Run the **display portal user all** command to check that the number of online portal users is 0.
2. Use the command **display portal server** to check the portal service status on the AC to be UP, indicating that the configuration is okay and the function is enabled.
3. Check the portal free-rule configuration, delete all portal free-rule rules and only retain two rules to the DNS server and to the portal server. The test found that redirection still cannot be achieved, and it can be directly connected to the external network.
4. Portal escape configuration is suspected to have been configured on AC before. All rules will be released on AP after local forwarding portal escape without portal authentication. Log in to the AP and use the **display portal rule all** command to view the portal rule currently issued to the AP. It is found that in addition to the DNS and IMC address permits, all source addresses to all destinations 80 and 443 are redirected, and other ports are denied. That the portal rule is okay. I also tried to restart the AP so that the AC reissued the portal rule configuration to the AP, but the problem remained.
5. It is suspected that the AP cannot communicate with the portal server or cannot resolve the portal url address to the portal server address, causing the AP to think that the server is blocked and escape, try to log in to the AP to configure the DNS address, AP can ping DNS, and ping the portal server IP address can also be connected. Indicates that the AP resolves the portal URL address and connectivity to the portal server is OK.
6. Try to reproduce the problem and visit the web page after connecting to the wireless connection. During this process, the debug information is collected on the AC and AP, and it is found that there is no redirected debug print, indicating that the portal function does not take effect.
7. Finally, go back to check the configuration for any suspicious configuration and modify it. It is found that the business vlan ID configured under the service template is inconsistent with the vlan ID specified for local forwarding, as follows:

```
# wlan service-template 1
ssid XXX
vlan XX1
client forwarding-location ap vlan XX2
portal enable method direct
portal domain xxx
portal bas-ip X.X.X.X
portal apply web-server portal
service-template enable
#
```

From the above configuration, it can be seen that the actual business VLAN is XX1, and the VLAN with local forwarding enabled is XX2. The **display wlan client** command on the AC shows that the terminal access is all on vlan XX1. The above configuration actually takes effect:

- 1) The actual vlan XX1 is centralized forwarding instead of local forwarding. Only the business of vlan XX2 is local forwarding, and the service template in the AP view is not configured with a vlan ID, so the actual business vlan is the business vlan XX1 configured under the service template.
- 2) The portal authentication configured under the service template can only be enabled in one forwarding mode, that is, either centralized forwarding or local forwarding. The two forwarding methods can not be enabled at the same time.
- 3) When the local forwarding command (**client forwarding-location ap**) is configured under the servi

ce template, regardless of whether the local forwarding vlan is specified or not, the portal can only be enabled under the local forwarding service.

Combining the above three elements, it finally shows that the actual business VLAN of this configuration method is centralized forwarding and the portal authentication function is not enabled.

Solution

1. Modify the local forwarding VLAN configuration to the actual business VLAN
2. Delete the local forwarding specified vlan configuration

```
# wlan service-template 1
```

```
ssid XXX
```

```
vlan XX1
```

```
client forwarding-location ap vlan XX1 or client forwarding-location ap
```

```
portal enable method direct
```

```
portal domain xxx
```

```
portal bas-ip X.X.X.X
```

```
portal apply web-server portal
```

```
service-template enable
```

```
#
```