Example for Configuring CWA Authentication

Networking Requirements

As shown in **Figure 1**, the terminals in the visitor area are connected to the company's internal network through the Switch. Unauthorized access to the internal network can damage the company's service system and cause leakage of key information assets. Therefore, the administrator employs the CWA on the Switch and on the Web Authentication Server of the AAA to control the users' network access rights to ensure internal network security.

Prerequisite

Ensure that PICA8 Switch is properly connected to the AAA server. In this example, the switch uses the management port Eth0 to connect to the AAA server.

Configuration on the AAA Server

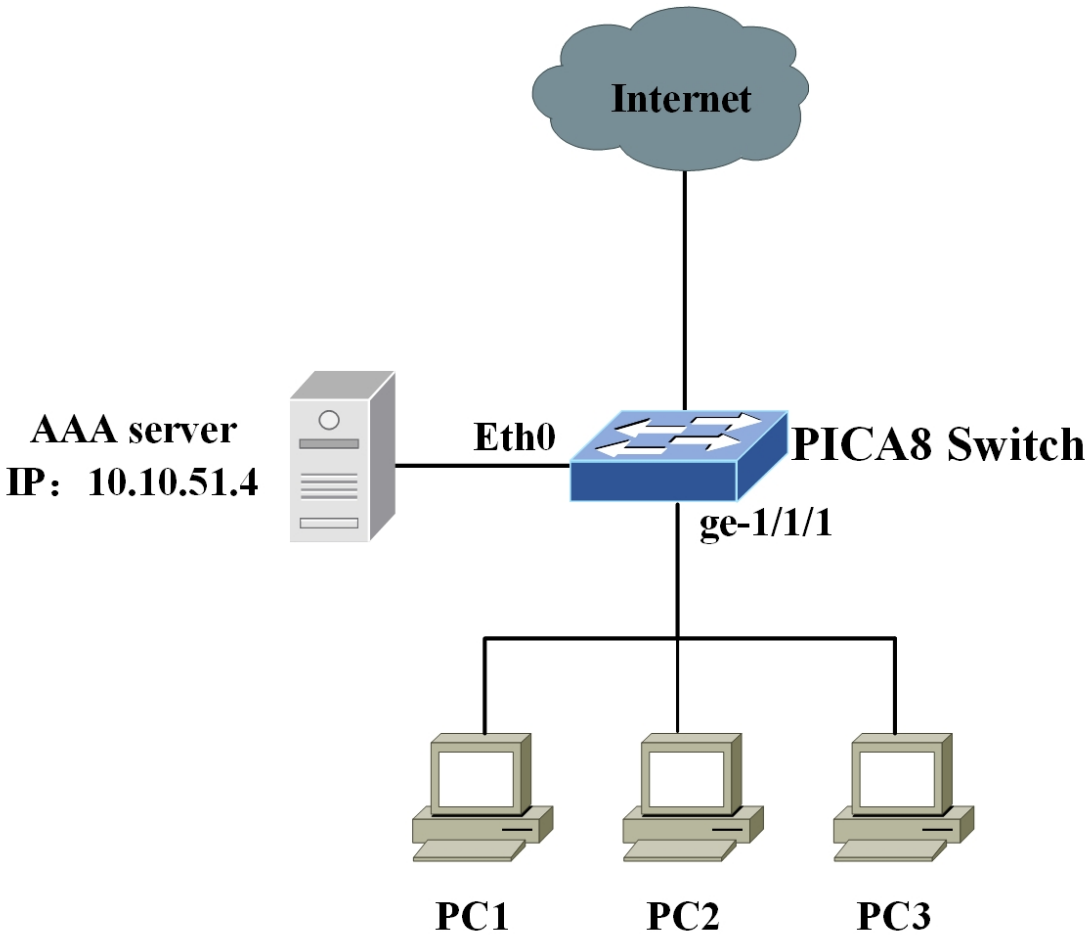
The configuration roadmap on the Web Authentication Server is as follows. For details, refer to the solution document Configuring Pica8 Switches with ClearPass Guest Central Web Authentication in Typical Configuration of NAC.

- Configure the Eth0 IP address of the switch to establish a connection to the switch.
- Configure the username and password on the AAA server for Web authentication.
- Configure a dynamic VLAN which is used to access the network normally after the user successfully authenticates.
- Configure other Web authentication attributes for Web authentication.

Configuration on the Switch

- Configure the 802.1X authentication server and Web authentication server on the Switch.
- The Web authentication process relies on MAB authentication. If you want to deploy Web authentication, enable MAB authentication on the switch first.
- Configure block VLAN and dynamic VLAN.
- Configure CoA authorization client.

Figure 1. Networking Diagram for Configuring CWA Authentication



Procedure

Step1 Configure the access port to trunk mode.

```
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
```

Step2 Configure the MAB and Web authentication modes. The Web authentication process relies on MAB authentication. If you want to deploy Web authentication, enable MAB authentication on the switch first.

```
admin@XorPlus# set protocols dot1x interface ge-1/1/1 auth-mode mac-radius
admin@XorPlus# set protocols dot1x interface ge-1/1/1 auth-mode web
```

Step3 Configure IP address of RADIUS server and the DNS server.

```
admin@XorPlus# set protocols dot1x aaa radius authentication server-ip 10.10.51.4 shared-key pica8
admin@Xorplus# set system dns-server-ip 192.168.10.1
```

NOTE:

- Configuring DNS server IP is required for CWA authentication.
- Make sure to configure the mapping of the domain name of the redirect URL to the IP address on the DNS server.

Step4 Configure the NAS IP address to the IP address of Eth0 interface which is connected to the AAA server.

```
admin@XorPlus# set protocols dot1x aaa radius nas-ip 10.10.51.100
```

This command is used to set the nas-ip field in RADIUS access-request message. If you use the management interface eth0/eth1 to connect to the RADIUS server, the IP address of the management interface eth0/eth1 should be used for the NAS IP address configured here.

Step5 Configure block VLAN. This step is required for Web authentication.

```
admin@XorPlus# set protocols dot1x block-vlan-id 10
admin@XorPlus# set interface gigabit-ethernet ge-1/1/1 family ethernet-switching port-mode trunk
admin@XorPlus# set interface gigabit-ethernet ge-1/1/2 family ethernet-switching native-vlan-id 10
admin@XorPlus# set vlans vlan-id 10 l3-interface vlan10
admin@XorPlus# set l3-interface vlan-interface vlan10 address 10.10.51.10 prefix-length 24
```

Step6 Configure a RADIUS dynamic authorization client from which the switch accepts Change of Authorization (CoA) messages. This step is required for CoA and Web authentication.

```
admin@Xorplus# set protocols dot1x aaa radius dynamic-author client 10.10.10.1 shared-key pica8123
```

Step7 Configure the host mode for NAC authentication interface.

```
admin@XorPlus# set protocols dot1x interface ge-1/1/1 host-mode multiple
```

Step8 Commit the configuration.

```
admin@Xorplus# commit
```

Step9 Verify the configuration.

a) Run the **run show dot1x interface** or **run show dot1x interface gigabit-ethernet** <*interface-name*> to check the CWA authentication configurations. The command output (**WEB = enable**) shows that the CWA authentication has been enabled on the interface ge-1/1/1 and MAC address 10:11:01:39:1a:00 is successfully authenticated.

```
admin@Xorplus# run show dot1x interface
Interface  802.1x   MAC-RADIUS  WEB   HOST-MODE   CLIENT-MAC  CLIENT-STATUS
--------------------------------------------------------------------------------
ge-1/1/1  disable  enable   enable   multiple  10:11:01:39:1a:00  authorized
                                              a1:31:a1:b9:6a:0c  authorized
                                              a2:e1:55:78:1a:33  authorized

admin@Xorplus# run show dot1x interface gigabit-ethernet ge-1/1/1
Interface ge-1/1/1:
============================================================
  Client MAC               : 10:11:01:39:1a:00
  Status                    : authorized
  Success Auth Method       : MAB
  Dynamic VLAN ID          : 100 (active)
============================================================
  Client MAC                  : a1:31:a1:b9:6a:0c
  Status                       : authorized
  Success Auth Method           : MAB
  Dynamic VLAN ID             : 100 (active)
============================================================
  Client MAC                  : a2:e1:55:78:1a:33
  Status                       : authorized
  Success Auth Method           : MAB
  Dynamic VLAN ID             : 100 (active)
============================================================
```

b) After starting the browser and entering any Web address, the user is redirected to the Web authentication login page. The user then enters the user name and password for authentication.

c) If the user name and password are correct, an authentication success message is displayed on the Web authentication page. The user can then access the network.