CWA URL Redirect support on C891FW

Introduction

The concept of central web authentication is opposed to local web authentication, which is the usual web authentication on the router itself. In that system, upon dot1x/mab failure, the router will failover to the webauth profile and will redirect client traffic to a web page on the router.

Central web authentication offers the possibility to have a central device that acts as a web portal (ISE). The major difference compared to the usual local web authentication is that it is shifted to Layer 2 along with mac/dot1x authentication. The concept also differs in that the radius server (ISE) returns special attributes that indicate to the router that a web redirection must occur. This solution has the advantage to eliminate any delay that was necessary for web authentication to kick. Globally, if the MAC address of the client station is not known by the radius server (but other criteria can also be used), the server returns redirection attributes, and the router authorizes the station (via MAC authentication bypass [MAB]) but places an access list to redirect the web traffic to the portal. Once the user logs in on the guest portal, it is possible via CoA (Change of Authorization) to bounce the router port so that a new Layer 2 MAB authentication occurs. The ISE can then remember it was a webauth user and apply Layer 2 attributes (like dynamic VAN assignment) to the user. An ActiveX component can also force the client PC to refresh its IP address.

This document describes how to configure central web authentication with wired clients connected to routers with the help of Identity Services Engine (ISE).

Prerequisites for CWA URL Redirect support on C891FW

Requirements

- Identity Services Engine (ISE)
- Cisco IOS router configuration

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Services Engine (ISE), Release 1.1.1

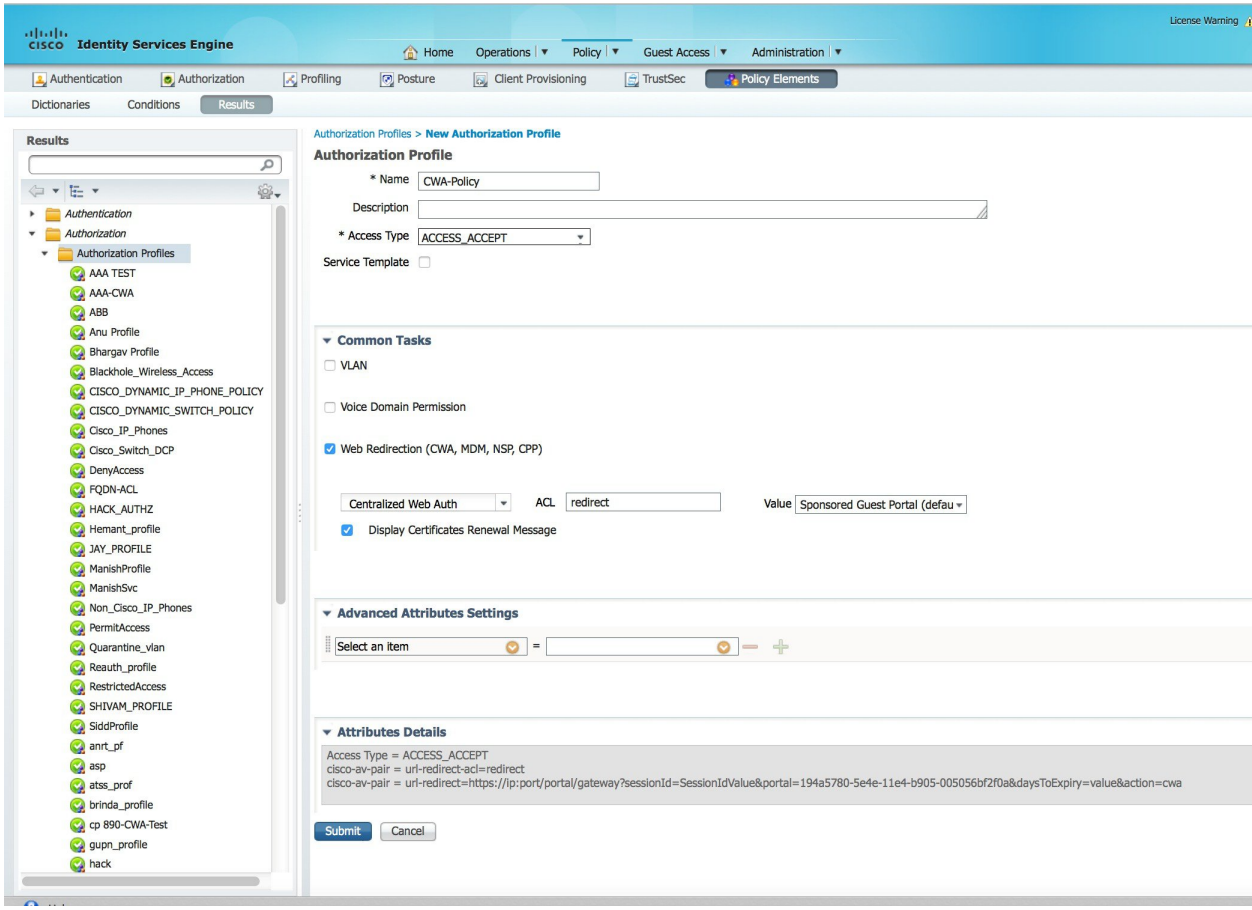
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuring CWA URL Redirect support on C891FW

Create an Authorization profile

The screenshot below displays the Authorization Profile configuration user interface:

Figure 1: Authorization Profile



1. Click **Policy**, and click **Policy Elements**.
2. Click **Results**.
3. Expand **Authorization**, and click **Authorization profile**.
4. Click the **Add** button in order to create a new authorization profile for central webauth.
5. In the **Name** field, enter a name for the profile.
6. Choose **ACCESS_ACCEPT** from the Access Type drop-down list.
7. Check the **Web Authentication** check box, and choose **Centralized** from the drop-down list.
8. In the **ACL** field, enter the name of the ACL on the switch that defines the traffic to be redirected.

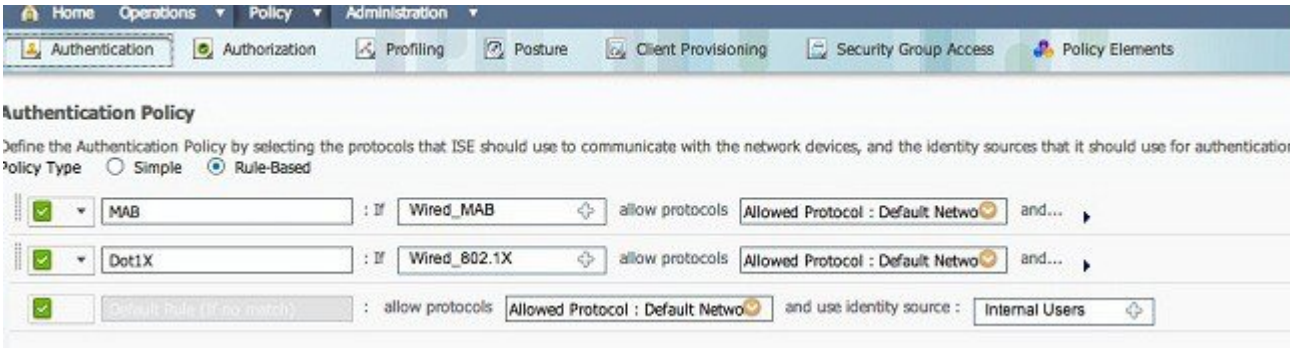
9 Choose **Default** from the Redirect drop-down list.

The Redirect attribute defines whether the ISE sees the default web portal or a custom web portal that the ISE admin created. For example, the redirect ACL in this example triggers a redirection upon HTTP or HTTPS traffic from the client to anywhere. The ACL is defined on the switch later in this configuration example.

Create an Authentication Rule

The screenshot below displays the Authorization Profile configuration user interface:

Figure 2: Authentication Rule



1 Under the Policy menu, click **Authentication**.

The following image shows an example of how to configure the authentication policy rule. In this example, a rule is configured that triggers when MAB is detected.

2 Enter a name for your authentication rule.

3 Select the plus **(+)** icon in the **If** condition field.

4 Select **Compound condition**, and then select **Wired_MAB**.

5 Click the arrow located next to **and ...** to expand the rule.

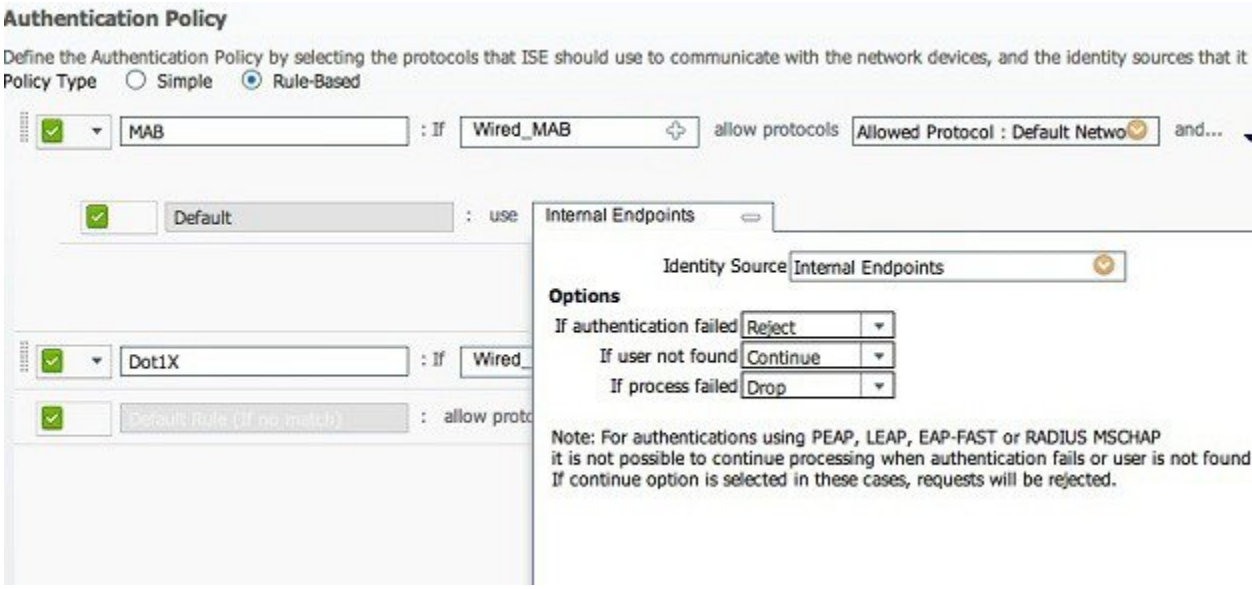
6 Click the + icon in the Identity Source field, and select **Internal endpoints**.

7 Select **Continue** from the If user not found drop-down list.

This option allows a device to be authenticated (through webauth) even if its MAC address is not known. Dot1x clients can still authenticate with their credentials and should not be concerned with this configuration.

The screenshot below displays the Internal Endpoints user interface:

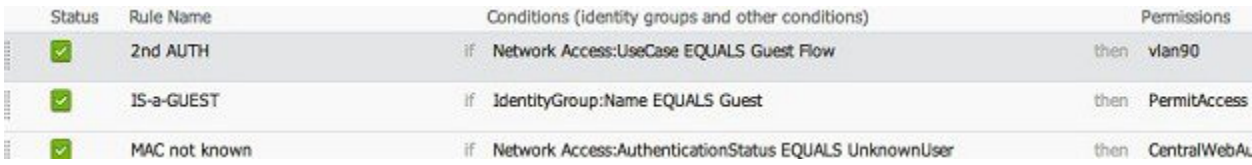
Figure 3: Authentication Rule-Internal Endpoints



Create an Authorization Rule

Note There are several rules to configure in the authorization policy. When the PC is plugged in, it goes through MAB; it is assumed that the MAC address is not known, so the webauth and ACL are returned. This MAC not known rule is shown in the following image and is configured in this section:

Figure 4: Authorization Rule



1. Create a new rule, and enter a name.
2. Click the plus **(+)** icon in the condition field, and select **create a new condition**.
3. Select **Expression** from the drop-down list.
4. Select **Network Access** and expand.
5. Click **AuthenticationStatus**, and select **Equals** operator.
6. Select **UnknownUser**.
7. On the General Authorization page, select **CentralWebauth**.

Note This step allows the ISE to continue even though the user (or the MAC) is not known. Unknown users are now presented with the Login page. However, once they enter their credentials, they are presented again with an authentication request on the ISE; therefore, another rule must be configured with a condition that is met if the user is a guest user. In this example, If UseridentityGroup equals Guest is used, and it is assumed that all guests belong to this group.

8 Click the **actions** button located at the end of the MAC not known rule, and choose to insert a new rule above.

Note It is very important that this new rule comes before the MAC not known rule.

9 Enter a name for the new rule. Example, *IS-a-GUEST*.

10 Choose a condition that matches your guest users. Example, *InternalUser:IdentityGroup Equals Guest*. This is because all guest users are bound to the Guest group (or another group you configured in your sponsor settings).

11 Select **PermitAccess** in the result box (located to the right of the word then).

When the user is authorized on the Login page, ISE restarts a Layer 2 authentication on the switch port, and a new MAB occurs. In this scenario, the difference is that an invisible flag is set for ISE to remember that it was a guest-authenticated user. This rule is 2nd AUTH, and the condition is Network Access:UseCase Equals GuestFlow. This condition is met when the user authenticates via webauth, and the switch port is set again for a new MAB. You can assign any attributes you like. This example assigns a profile vlan90 so that the user is assigned the VLAN 90 in his second MAB authentication.

12 Click **Actions** (located at the end of the IS-a-GUEST rule), and select **Insert new rule above**.

13 Enter **2nd AUTH** in the name field.

14 In the condition field, click the **(+)** icon, and choose to create a new condition.

15 Select **Network Access**, and select **UseCase**.

16 Select **Equals** as the operator.

17 Select **GuestFlow** as the right operand.

18 On the authorization page, click the **(+)** icon to select a result for your rule.

In this example, a preconfigured profile (vlan90) is assigned; this configuration is not shown in this document.

Note You can use the **Permit Access** option or create a custom profile in order to return the VLAN or attributes.

Enable the IP Renewal

Note This task is optional.

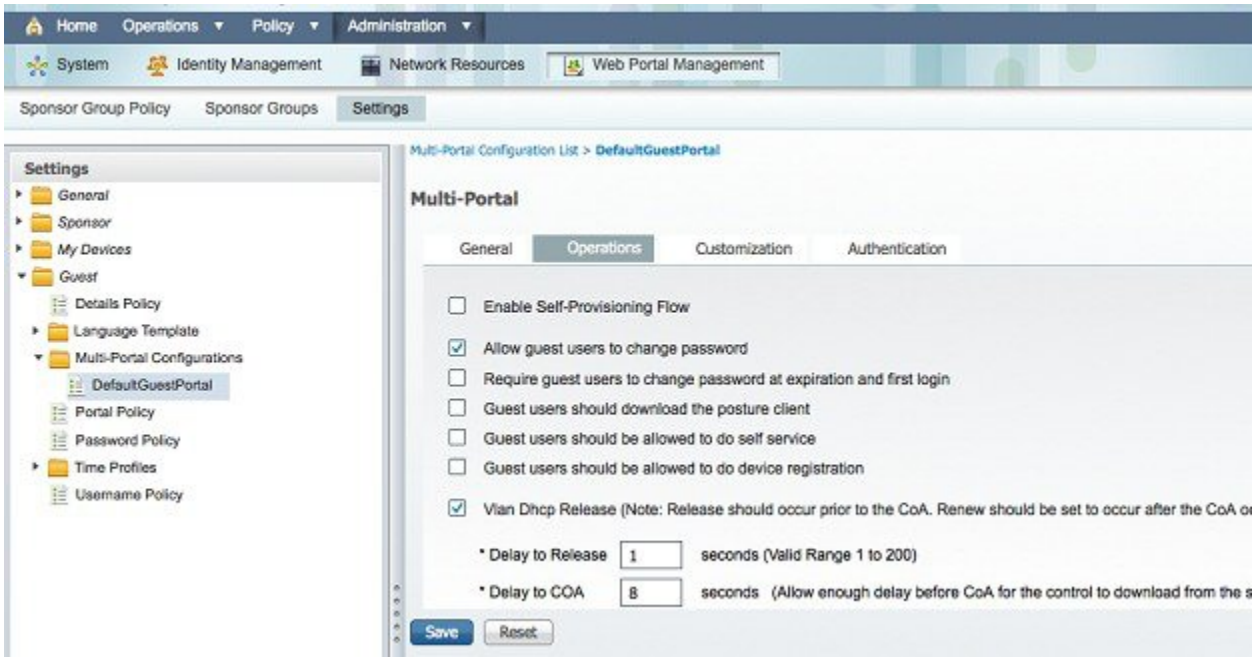
If you assign a VLAN, the final step is for the client PC to renew its IP address. This step is achieved by the guest portal for Windows clients. If you did not set a VLAN for the 2nd AUTH rule earlier, you can skip this task.

1. Click **Administration**, and select **Guest Management**.
2. Click **Settings**.
3. Select **Guest**, and expand **Multi-Portal Configuration**.
4. Click **DefaultGuestPortal** or the name of the custom portal you have created.
5. Select the **Vlan DHCP Release** check box.

Note This option works only for Windows clients.

The following screenshot displays the IP Renewal user interface:

Figure 5: IP Renewal



Task Result

The client PC plugs in and performs MAB. The MAC address is not known, so ISE pushes the redirection attributes back to the router. The user tries to go to a website and is redirected.

When the authentication of the Login page is successful, the ISE bounces the switchport through Change Of Authorization, which starts again a Layer 2 MAB authentication.

However, the ISE knows that it is a former webauth client and authorizes the client based on the webauth credentials (although this is a Layer 2 authentication).

In the ISE authentication logs, the MAB authentication appears at the bottom of the log. Although it is unknown, the MAC address was authenticated and profiled, and the webauth attributes were returned. Next, authentication occurs with the user's login credentials (at the Login page). Immediately after authentication, a new Layer 2 authentication occurs with the username as credentials; this authentication step is where you can return attributes such dynamic VLAN.

HTTP Proxy Configuration

If you use an HTTP proxy for your clients, it means that your clients:

- Use a unconventional port for HTTP protocol.
- Send all their traffic to that proxy.

You can use the **ip http port** command and the **ip port-map http port** command to enable the router to listen to specific ports.

You also need to configure all clients to keep using their proxy but to not use the proxy for the ISE IP address. All browsers include a feature that allows you to enter host names or IP addresses that should not use the proxy. If you do not add the exception for the ISE, you encounter a loop authentication page.

You also need to modify your redirection ACL to permit on the proxy port.

Configuration Examples for CWA URL Redirect support on C891FW

Example: MAB Configuration

```
enable
Configure terminal
interface GigabitEthernet 4
 switchport access vlan 5
 no ip address
 authentication order mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 mab
 spanning-tree portfast
 end
```

Example: ACL Configuration

VLAN 100 is the VLAN that provides full network connectivity. A default port ACL (named webauth) is applied and defined as shown here:

```
ip access-list extended webauth
permit ip any any
```

This sample configuration gives full network access even if the user is not authenticated; therefore, you might want to restrict access to unauthenticated users.

In this following configuration, HTTP and HTTPS browsing does not work without authentication (per the other ACL) since ISE is configured to use a redirect ACL (named redirect).

```
ip access-list extended redirect
deny udp any any eq domain
deny tcp any any eq domain
```

```
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny ip any host <ISE ip address>
permit tcp any any eq www
permit tcp any any eq 443
```

This access list must be defined on the router in order to define on which traffic the router will perform the redirection. (It matches on permit.) In this example, any HTTP or HTTPS traffic that the client sends triggers a web redirection. This example also denies the ISE IP address so traffic to the ISE goes to the ISE and does not redirect in a loop. (In this scenario, deny does not block the traffic; it just does not redirect the traffic.) If you use unusual HTTP ports or a proxy, you can add other ports.

You can also allow HTTP access to some web sites and redirect other websites. For example, if you define in the ACL a permit for internal web servers only, clients could browse the web without authenticating but would encounter the redirect if they try to access an internal web server.

You must allow the CoA on the router since ISE cannot force the switch to re-authenticate the client. To allow CoA:

```
aaa server radius dynamic-author
     client <ISE ip address> server-key <radius shared secret>
```

You can use the **ip http server** command to redirect based on HTTP traffic and **ip http secure-server** command to redirect based on HTTPS traffic.

Example: Verifying user authentication

You can use the **show authentication session int <interface num>** command to check if the user is authenticated. The following example shows a sample output of the **show authentication session int <interface num>** command when the user is not authenticated.

```
Device#show auth sess int gi1/0/12
           Interface:  GigabitEthernet1/0/12
         MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
                       sessionId=C0A82102000002D8489E0E84&action=cwa
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

       Method   State
       mab      Authc Success
```

Note Despite a successful MAB authentication, the redirect ACL is placed since the MAC address was not known by the ISE.

Example: Router Configuration

This section lists the full router configuration. Some unnecessary interfaces and command lines have been omitted; therefore, this sample configuration should be used for reference only and should not be copied.

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname autonet-4
!
boot-start-marker
boot system flash:c800-universalk9-mz.SSA.156-2.24.T
boot system flash:c800-universalk9-mz.SSA.156-2.19.T
boot-end-marker
!
!
logging buffered 30000000
enable password lab
!
aaa new-model
!
!
aaa authentication login NO_LOGIN none
aaa authentication dot1x default group radius
aaa authorization network default group radius
!
!
!
!
aaa server radius dynamic-author
 client 20.0.0.1 server-key cisco123
!
aaa session-id common
ethernet lmi ce
!
!
!
!
!
!
!
!
device-sensor filter-list cdp list CDP_FILTER
 tlv name address-type
 tlv number 10
device-sensor filter-spec cdp include list CDP_FILTER
device-sensor accounting
device-sensor notify all-changes
ip auth-proxy inactivity-timer 5
ip admission inactivity-timer 5
ip admission name CWA_TEST consent inactivity-time 5 absolute-timer 10
!
!
!
!
!
!
!
!
!
!
!


!
!
!
!
```

```
no ip domain lookup
ip inspect WAAS flush-timeout 10
ip device tracking
ip cef
ipv6 unicast-routing
ipv6 cef
ntp max-associations 1000
!
!
!
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
license udi pid C892FSP-K9 sn FTX192680ZR
!
!
username CISCO privilege 0 password 0 cisco
!
redundancy
 notification-timer 120000
!
!
!
autonomic
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0
 no ip address
!
interface GigabitEthernet1
 switchport access vlan 3
 no ip address
!
interface GigabitEthernet2
 switchport access vlan 2
 no ip address
!
interface GigabitEthernet3
 switchport access vlan 4
 no ip address
!
interface GigabitEthernet4
 switchport access vlan 5
 no ip address
 authentication order mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 mab
 spanning-tree portfast
!
interface GigabitEthernet5
 no ip address
!
interface GigabitEthernet6
```

```
 switchport access vlan 6
 no ip address
!
interface GigabitEthernet7
 switchport access vlan 7
 no ip address
!
interface GigabitEthernet8
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet9
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Vlan1
 ip address 126.53.1.4 255.255.255.0
 authentication host-mode multi-host
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 120
 authentication timer reauthenticate 600
 authentication fallback TEST
 mab
!
interface Vlan2
 no ip address
 authentication host-mode multi-host
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 120
 authentication timer reauthenticate 600
 authentication fallback TEST
 mab
!
interface Vlan3
 no ip address
 authentication host-mode multi-host
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 120
 authentication timer reauthenticate 600
 authentication fallback TEST
 mab
!
interface Vlan4
 no ip address
 authentication host-mode multi-host
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 120
 authentication timer reauthenticate 600
 authentication fallback TEST
 mab
!
interface Vlan5
 ip address 10.0.0.4 255.255.255.0
!
interface Vlan6
 ip address 20.0.0.4 255.255.255.0
 authentication host-mode multi-host
```

```
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 120
 authentication timer reauthenticate 600
 authentication fallback TEST
 mab
!
interface Vlan7
 ip address 30.0.0.4 255.255.255.0
 authentication host-mode multi-host
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 120
 authentication timer reauthenticate 600
 authentication fallback TEST
 mab
!
ip default-gateway 126.53.1.254
ip forward-protocol nd
ip http server
no ip http secure-server
ip http max-connections 10
!
!
ip nat pool inside-pool-2 16.1.1.1 16.1.1.1 prefix-length 24
ip route 0.0.0.0 0.0.0.0 126.53.1.254
!
ip access-list extended redirect
 deny   ip any host 20.0.0.1
 permit tcp any any eq www
 permit tcp any any eq 443
!
ipv6 ioam timestamp
!
access-list 2 permit 60.1.1.0 0.0.0.255
access-list 2 permit 60.0.0.0 0.0.0.255
!
radius server host
 address ipv4 20.0.0.1 auth-port 1812 acct-port 1813
 key cisco123
!
!
!
control-plane
!
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 no modem enable
line aux 0
line vty 0 4
 length 0
 transport input all
!
scheduler allocate 20000 1000
```

```
!
end
```

Example: HTTP Proxy Configuration

The following example shows how to configure the proxy port to 8080:

```
enable
configure terminal
ip http port 8080
ip port-map http port 8080
```

Important Notes

Important Note about Router SVIs

The router needs a switch virtual interface (SVI) in order to reply to the client and send the web portal redirection to the client. This SVI does not necessarily have to be on the client subnet/VLAN. However, if the router has no SVI in the client subnet/VLAN, it has to use any of the other SVIs and send traffic as defined in the client routing table. This typically means traffic is sent to another gateway in the core of the network; this traffic comes back to the access switch inside the client subnet.

Firewalls typically block traffic from and to the same router, as in this scenario, so redirection might not work properly. You can allow this behavior on the firewall or create an SVI on the access router in the client subnet.

Important Note about HTTPS Redirection

Routers are able to redirect HTTPS traffic. If the guest client has a homepage in HTTPS, the redirection occurs correctly.

The whole concept of redirection is based upon the fact that a device (in this case, the router) replaces the website IP address. However, a major issue arises when the router intercepts and redirects HTTPS traffic because the router can present only its own certificate in the Transport Layer Security (TLS) handshake. Since this is not the same certificate as the website originally requested, most browsers issue major alerts. The browsers correctly handle the redirection and presentation of another certificate as a security concern. There is no solution for this, you cannot use the router to replace your original website certificate.

Additional References for CWA URL Redirect support on C891FW

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for CWA URL Redirect support on C891FW

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for CWA URL Redirect support on C891FW

Feature Name	Releases	Feature Information
CWA URL Redirect support on C891FW	15.6(3)M	CWA URL Redirect support on C891FW feature enables you to manage Central Web Authentication (CWA) URL redirects to Identity Services Engine (ISE) or other websites. No commands were introduced or modified by this feature.