aruba
a Hewlett Packard Enterprise company

L2 GRE for Guest Access in ArubaOS8

Technote

Copyright Information

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

www.arubanetworks.com

3333 Scott Blvd

Santa Clara, CA 95054

Phone: 1-800-WIFI-LAN (+800-943-4526)

Fax 408.227.4550

Contents

Revision History 4
About this Guide 5
Overview 5
Related Documents 5
Acronym List 5
Introduction 6
Topology 7
Common Configuration 8
Assumptions 8
DMZ side Configuration 8
Campus side Configuration 13
Configuration required on Clearpass for Guest Authentication 15
ClearPass Policy Manager Configuration 15
ClearPass Guest Configuration 20
Configuring L2 GRE 23
Option 1: Configuring L2 GRE tunnels from each individual Campus MCs to DMZ MCs 23
Assumptions 23
Configuration 23
Option 2: Configuring a single L2 GRE tunnel from the VIP of Campus MCs to DMZ MCs 25
Assumptions 25
Configuration 25

Revision History

The following table lists the revisions of this document:

Revision	Change Description
Revision 1	Initial Publication

Table 1 *Revision History*

About this Guide

Overview

This document explains two scenarios while deploying L2 GRE for Guest access and steps to configure the same on ArubaOS 8. It assumes that the wireless network is deployed using standard Aruba design practices. The intended audience for this document is the network administrators who want to implement secure guest access solution with captive portal authentication between clusters of Mobility Controllers in the Campus network with the DMZ Mobility Controllers.

Related Documents

ArubaOS 8.7.0.x User Guide

ArubaOS 8 Fundamentals Guide

ArubaOS 8 CLI Reference Guide

ArubaOS 8 Base Design Lab Guide

Acronym List

Acronym	Definition
MCR	Mobility Conductor (Old name: MM or Mobility Master)
MC	Mobility Controller
AP	Access Point
CLI	Command Line Interface
VIP	Virtual IP
DMZ	Demilitarized Zone

Introduction

To keep the guest traffic isolated from the corporate network, it is recommended to deploy MCs in DMZ to handle all the guest user authentication, captive portal, IP addressing and data traffic management.

This would mean that WLAN configuration of the Guest network would reside on Campus MCs and the clients would connect to APs on Campus side but all the traffic would be tunneled to the DMZ. A Guest VLAN will be created on MCs which will not be present anywhere else on the corporate network and this VLAN will be extended to DMZ through L2 GRE tunnels. This will keep the guest traffic isolated from the corporate network.

Multizone is another feature which could be used for configuring guest access and multi-tenancy, however this document focuses on L2 GRE concept and configuration.

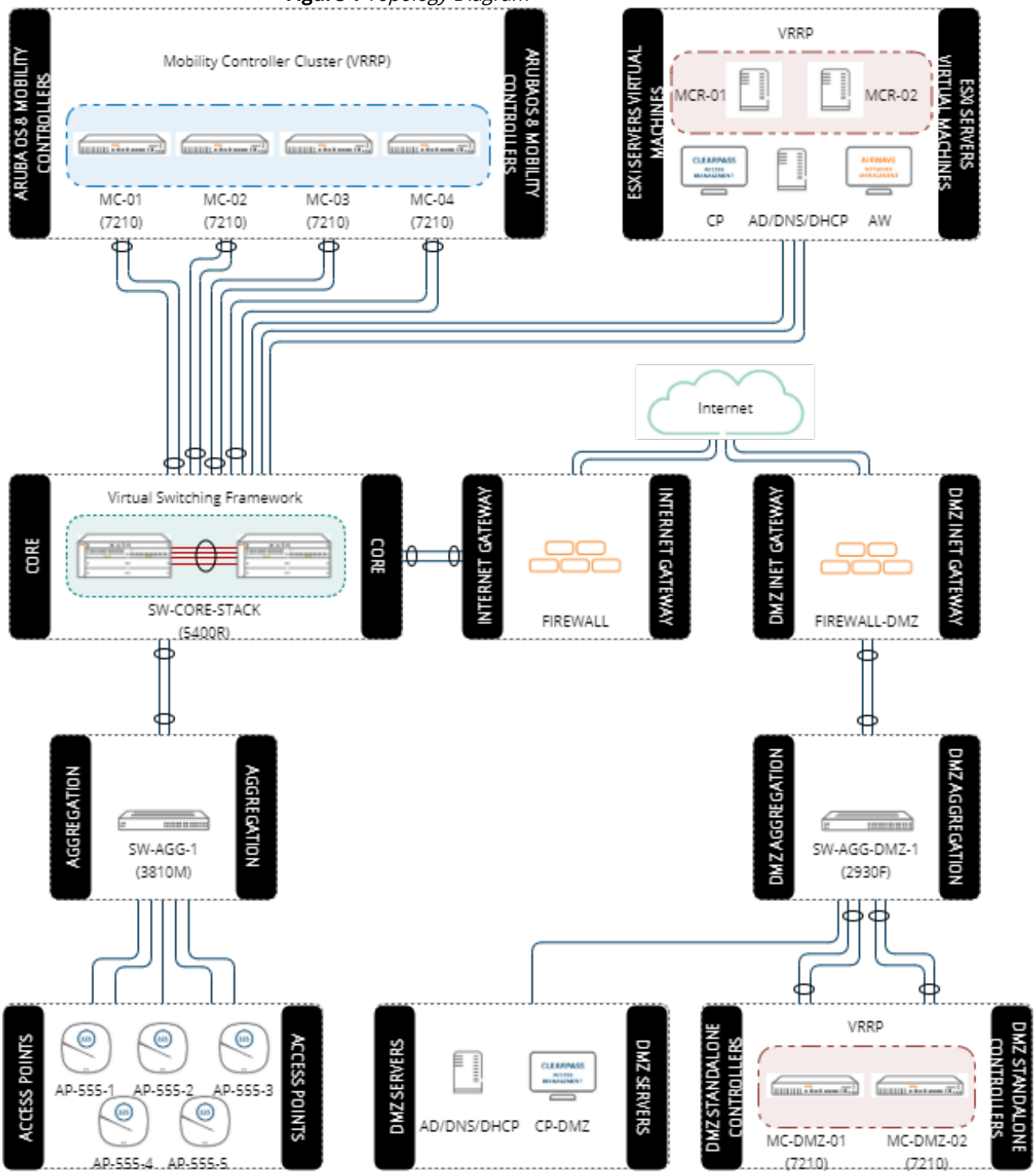
There are two ways to configure the GRE tunnels which are described in this document:

- Configuring tunnels from each individual Campus controller to DMZ controllers
- Configuring a single tunnel from Campus controllers to DMZ controllers.

Topology

This is lab network topology used to validate the configuration described throughout this document.

Figure 1 *Topology Diagram*



Common Configuration

Assumptions

- The configuration shown below is with respect to the topology shown in the above diagram.
- There are 4 MCs on the Campus side in cluster and 2 MCs on the DMZ side which are standalone MCs configured with a VRRP in L2 redundancy.
- The node-hierarchy on the Campus side: root>md>Aruba>Campus>4 MCs(mc01, mc02, mc03, mc04)

DMZ side Configuration

Creating a new guest VLAN 999 for all the guest traffic.

Create a Guest VLAN on Firewall/Router on DMZ side

Create a Guest VLAN 999 on the Firewall/Router in DMZ with IP address: 192.168.1.1 255.255.255.0

Create a Guest VLAN on uplink switch of DMZ MCs

```
SW-AGG-DMZ #conf t
SW-AGG-DMZ(config)# vlan <999>
SW-AGG-DMZ(vlan-999)# name <999-GuestClients>
SW-AGG-DMZ(vlan-999)# ip address <192.168.1.2> <255.255.255.0>
SW-AGG-DMZ(vlan-999)# save
```

Create a Guest VLAN on DMZ MCs

```
(mc-dmz01) [mynode] #conf t
(mc-dmz01) [mynode] (config) #vlan <999>
(mc-dmz01) [mynode] (config-submode)#exit
(mc-dmz01) [mynode] (config) #vlan-name <GuestVLAN>
(mc-dmz01) [mynode] (config) #vlan GuestVLAN 999
(mc-dmz01) [mynode] (config) #interface vlan 999
(mc-dmz01) [mynode] (config-submode)#ip address <192.168.1.11> <255.255.255.0>
(mc-dmz01) [mynode] (config-submode)#exit

(mc-dmz01) [mynode] (config) #interface vlan 10          (This is the vlan which holds the controller-IP)
(mc-dmz01) [mynode] (config-submode)#ip nat outside      (Configured to achieve successful communication of return traffic from ClearPass guest page)
(mc-dmz01) [mynode] (config-submode)#write memory
```

```
(mc-dmz02) [mynode] #conf t
(mc-dmz02) [mynode] (config) #vlan <999>
(mc-dmz02) [mynode] (config-submode)#exit
(mc-dmz02) [mynode] (config) #vlan-name <GuestVLAN>
(mc-dmz02) [mynode] (config) #vlan GuestVLAN 999
(mc-dmz02) [mynode] (config) #interface vlan 999
(mc-dmz02) [mynode] (config-submode)#ip address <192.168.1.12> <255.255.255.0>
(mc-dmz02) [mynode] (config-submode)#exit

(mc-dmz01) [mynode] (config) #interface vlan 10          (This is the vlan which holds the controller-IP)
(mc-dmz01) [mynode] (config-submode)#ip nat outside      (Configured to achieve successful communication of return traffic from ClearPass guest page)
(mc-dmz02) [mynode] (config-submode)#write memory
```

Make sure to allow this newly created vlan 999 on the uplink port/port-channel of the MC.

Create DHCP server on DMZ MCs

Typically, there will be dedicated DHCP server(s) in the DMZ for providing IP addresses to the guest devices (recommended). However if there is a need, DHCP can be set up on the MCs in the DMZ.

Mobility Controllers typically support around 4000 DHCP addresses depending on each model.

Configuring VIP to be used during DHCP server configuration:

```
(mc-dmz01) [mynode] #conf t
(mc-dmz01) [mynode] (config) # vrrp <192>
(mc-dmz01) [mynode] (config-submode) #ip address
<192.168.1.10>
(mc-dmz01) [mynode] (config-submode) #vlan 999
(mc-dmz01) [mynode] (config-submode) #priority 110
(mc-dmz01) [mynode] (config-submode) #no shutdown
(mc-dmz01) [mynode] (config-submode) #exit

(mc-dmz02) [mynode] #conf t
(mc-dmz02) [mynode] (config) # vrrp <192>
(mc-dmz02) [mynode] (config-submode) #ip address
<192.168.1.10>
(mc-dmz02) [mynode] (config-submode) #vlan 999
(mc-dmz02) [mynode] (config-submode) #priority 100
(mc-dmz02) [mynode] (config-submode) #no shutdown
(mc-dmz02) [mynode] (config-submode) #exit
```

Configuring the DHCP server:

```
(mc-dmz01) [mynode] #conf t
(mc-dmz01) [mynode] (config) #ip dhcp pool guestnet
(mc-dmz01) [mynode] (config-submode)#default-router 192.168.1.10
(mc-dmz01) [mynode] (config-submode)#dns-server 10.20.30.40
(mc-dmz01) [mynode] (config-submode)#network 192.168.1.0 255.255.255.128
(mc-dmz01) [mynode] (config-submode)#write memory

(mc-dmz02) [mynode] #conf t
(mc-dmz02) [mynode] (config) #ip dhcp pool guestnet
(mc-dmz02) [mynode] (config-submode)#default-router 192.168.1.10
(mc-dmz02) [mynode] (config-submode)#dns-server 10.20.30.40
(mc-dmz02) [mynode] (config-submode)#network 192.168.1.128 255.255.255.128
(mc-dmz02) [mynode] (config-submode)#write memory
```

User role and Captive Portal Configuration

This section covers the standard configuration of user roles and captive portal for guest SSID.

```
(mc-dmz01) [mynode] (config) #cd /mm
```
(This will create the config at higher node level which can be inherited by the other MC)

```
(mc-dmz01) [mm] (config) #netdestination guest-dmz-external-captive-portal
(mc-dmz01) [mm] (config-submode) #host <CPPM-IP>
(mc-dmz01) [mm] (config-submode) #exit
```

Create alias for the captive portal

```
(mc-dmz01) [mm] (config) #netdestination guest-dmz-internal-net
(mc-dmz01) [mm] (config-submode) #network <10.0.0.0 255.0.0.0>
(mc-dmz01) [mm] (config-submode) #network <192.168.0.0 255.255.0.0>
(mc-dmz01) [mm] (config-submode) #exit
```

Create alias for the internal and DMZ network

```
(mc-dmz01) [mm] (config) #ip access-list session guest-dmz-allow-external-captive-portal
(mc-dmz01) [mm] (config-submode) #user alias guest-dmz-external-captive-portal svc-http permit
(mc-dmz01) [mm] (config-submode) #user alias guest-dmz-external-captive-portal svc-https permit
(mc-dmz01) [mm] (config-submode) #exit
```

Permit http and https traffic to captive portal

```
(mc-dmz01) [mm] (config) #ip access-list session guest-dmz-block
(mc-dmz01) [mm] (config-submode) #user alias guest-dmz-internal-net any deny
(mc-dmz01) [mm] (config-submode) #exit
```

Block client traffic to the internal network

```
(mc-dmz01) [mm] (config) #ip access-list session guest-dmz-cplog-out
(mc-dmz01) [mm] (config-submode) #user alias controller svc-https dst-nat 8081
(mc-dmz01) [mm] (config-submode) #exit
```

Permit redirect to controller after successful guest registration

```
(mc-dmz01) [mm] (config) #ip access-list session guest-dmz-authenticated
(mc-dmz01) [mm] (config-submode) #any any svc-http permit
(mc-dmz01) [mm] (config-submode) #any any svc-https permit
(mc-dmz01) [mm] (config-submode) #exit
```

Permit http and https traffic

```
(mc-dmz01) [mm] (config) #ip access-list session guest-dmz-drop-all
(mc-dmz01) [mm] (config-submode) #user any any deny log position 1
(mc-dmz01) [mm] (config-submode) #exit
```

Deny all traffic not explicitly permitted by other ACLs

```
(mc-dmz01) [mm] (config) #user-role guest-dmz
(mc-dmz01) [mm] (config-submode) #access-list session guest-dmz-cplogout position 3
(mc-dmz01) [mm] (config-submode) #access-list session logon-control position 4
(mc-dmz01) [mm] (config-submode) #access-list session guest-dmz-block position 5
(mc-dmz01) [mm] (config-submode) #access-list session guest-dmz-authenticated position 6
(mc-dmz01) [mm] (config-submode) #access-list session guest-dmz-drop-all position 7
(mc-dmz01) [mm] (config-submode) #exit
```

Create guest-dmz user role and apply ACLs

```
(mc-dmz01) [mm] (config) #user-role guest-dmz-logon
(mc-dmz01) [mm] (config-submode) #access-list session guest-dmz-allow-external-captive-portal position 3
(mc-dmz01) [mm] (config-submode) #access-list session logon-control position 4
(mc-dmz01) [mm] (config-submode) #access-list session captiveportal position 5
(mc-dmz01) [mm] (config-submode) #exit
```

Create guest-dmz-logon user role and apply ACLs

```
(mc-dmz01) [mm] (config) #aaa authentication-server radius CP-DMZ
(mc-dmz01) [mm] (RADIUS Server "CP-DMZ") #host <CPPM-IP>
(mc-dmz01) [mm] (RADIUS Server "CP-DMZ") #key <admin123>
(mc-dmz01) [mm] (RADIUS Server "CP-DMZ") #mac-delimiter colon
(mc-dmz01) [mm] (RADIUS Server "CP-DMZ") #exit
```

Designate RADIUS server

```
(mc-dmz01) [mm] (config) #aaa rfc-3576-server <CPPM-IP>
(mc-dmz01) [mm] (RFC 3576 Server " CPPM-IP") #key <admin123>
```

Designate RFC 3576 server

```
(mc-dmz01) [mm] (RFC 3576 Server " CPPM-IP") #exit
```

```
(mc-dmz01) [mm] (config) #aaa server-group CP-DMZ
(mc-dmz01) [mm] (Server Group "CP-DMZ") #auth-server CP-DMZ
(mc-dmz01) [mm] (Server Group "CP-DMZ") #exit
```

Define AAA server group

```
(mc-dmz01) [mm] (config) #aaa authentication mac guest-dmz
(mc-dmz01) [mm] (MAC Authentication Profile "guest-dmz") #delim-
iter colon
(mc-dmz01) [mm] (MAC Authentication Profile "guest-dmz") #case upper
(mc-dmz01) [mm] (MAC Authentication Profile "guest-dmz") #exit
```

Define MAC authentication profile

```
(mc-dmz01) [mm] (config) #aaa authentication captive-portal
guest-dmz
(mc-dmz01) [mm] (Captive Portal Authentication Profile "guest-dmz") #login-page https://
CPPM-IP/guest/guest_registration.php
```

Define captive portal profile

(This value: "guest_registration" should match the ClearPass Guest Self-Registration Page configuration. This is described in the next sections)

```
(mc-dmz01) [mm] (Captive Portal Authentication Profile "guest-dmz") #welcome-page
/auth/welcome.html
(mc-dmz01) [mm] (Captive Portal Authentication Profile "guest-dmz") #no guest-logon
(mc-dmz01) [mm] (Captive Portal Authentication Profile "guest-dmz") #redirect-pause 3
(mc-dmz01) [mm] (Captive Portal Authentication Profile "guest-dmz") #server-group CP-DMZ
(mc-dmz01) [mm] (Captive Portal Authentication Profile "guest-dmz") #default-role guest-
dmz-logon
(mc-dmz01) [mm] (Captive Portal Authentication Profile "guest-dmz") #exit
```

```
(mc-dmz01) [mm] (config) #user-role guest-dmz-logon
(mc-dmz01) [mm] (config-submode) #captive-portal guest-dmz
(mc-dmz01) [mm] (config-submode) #exit
```

Apply captive portal profile to the guest-dmz-logon role

```
(mc-dmz01) [mm] (config) #aaa profile guest-dmz
(mc-dmz01) [mm] (AAA Profile "guest-dmz") #initial-role guest-dmz-logon
(mc-dmz01) [mm] (AAA Profile "guest-dmz") #mac-default-role guest-dmz
(mc-dmz01) [mm] (AAA Profile "guest-dmz") #radius-accounting CP-DMZ
(mc-dmz01) [mm] (AAA Profile "guest-dmz") #rfc-3576-server <CPPM-IP>
(mc-dmz01) [mm] (AAA Profile "guest-dmz") #authentication-mac guest-dmz
(mc-dmz01) [mm] (AAA Profile "guest-dmz") #mac-server-group CP-DMZ
(mc-dmz01) [mm] (AAA Profile "guest-dmz") #exit
```

Define the AAA profile

Assign AAA profile to Wired Authentication Profile

The traffic coming in over the L2 GRE tunnel to the DMZ is considered wired traffic to the DMZ controllers. Hence we configure this wired authentication profile.

```
(mc-dmz01) [mynode] (config) #cd /mm
(mc-dmz01) [mm] (config) #aaa authentication wired
(mc-dmz01) [mm] (Wired Authentication Profile) #profile guest-dmz    (This AAA profile was created in the previous step)
(mc-dmz01) [mm] (Wired Authentication Profile) #write memory
```

Campus side Configuration

Create a Guest VLAN on Campus MCs

This guest VLAN will only be present on the MCs. This VLAN is unknown to the rest of the corporate network. Log in to your MM and navigate to your MC

```
(mcr01)#cd md>Aruba>Campus
(mcr01) [Campus] #conf t
(mcr01) [Campus] (config) #vlan <999>
(mcr01) [Campus] (config-submode)#exit
(mcr01) [Campus] (config) #vlan-name <GuestVLAN>
(mcr01) [Campus] (config) #vlan GuestVLAN 999
(mcr01) [Campus] (config) #write memory
```

Optionally configure interface IP addresses for each MC if granular control is required for troubleshooting

```
(mcr01)#cd mc01
(mcr01) [mc01] #conf t
(mcr01) [mc01] (config) #interface vlan 999
(mcr01) [mc01] (config-submode)#ip address <192.168.1.21> <255.255.255.0>
(mcr01) [mc01] (config-submode)#write memory

(mcr01)#cd mc02
(mcr01) [mc02] #conf t
(mcr01) [mc02] (config) #interface vlan 999
(mcr01) [mc02] (config-submode)#ip address <192.168.1.22> <255.255.255.0>
(mcr01) [mc02] (config-submode)#write memory
```

Similar configuration on MC3 and MC4

Make sure to allow this newly created vlan 999 on the uplink port/port-channel of the MC.

User Role and WLAN SSID Configuration

Configure allow-all user role and assign it to AAA profile

Allow all user role is created and assigned to the Guest SSID since we want all the unfiltered guest traffic to be sent to the DMZ and then actual roles with appropriate policies are assigned by the DMZ controller.

```
(mcr01)# cd /md/Aruba/Campus
(mcr01) [Campus] # conf t
(mcr01) [Campus] (config) # ip access-list session allowall-guest-acl
(mcr01) [Campus] (config-submode) #any any svc-http permit
(mcr01) [Campus] (config-submode) #any any svc-https permit
(mcr01) [Campus] (config-submode) # exit
(mcr01) [Campus] (config) # user-role guest-allowall
(mcr01) [Campus] (config-submode) # access-list session allowall-guest-acl position 1

(mcr01) [Campus] (config) #aaa profile Guest-SSID-AAA
(mcr01) [Campus] (AAA Profile "ABC") #initial-role guest-allowall
(mcr01) [Campus] (AAA Profile "ABC") #write memory
```

WLAN SSID Configuration

```
(mcr01) [Campus] (config) # wlan ssid-profile Guest-SSID
(mcr01) [Campus] (SSID Profile "Guest-SSID") #essid Guest-SSID
(mcr01) [Campus] (SSID Profile "Guest-SSID") #opmode opensystem
(mcr01) [Campus] (SSID Profile "Guest-SSID") #exit

(mcr01) [Campus] (config) #wlan virtual-ap Guest-SSID
(mcr01) [Campus] (Virtual AP profile "Guest-SSID") # aaa-profile Guest-SSID-AAA
(mcr01) [Campus] (Virtual AP profile "Guest-SSID") #ssid-profile Guest-SSID
(mcr01) [Campus] (Virtual AP profile "Guest-SSID") #vlan 999
(mcr01) [Campus] (Virtual AP profile "Guest-SSID") #exit

(mcr01) [Campus] (config) #ap-group CampusAP
(mcr01) [Campus] (AP group "CampusAP") #virtual-ap Guest-SSID
(mcr01) [Campus] (AP group "CampusAP") #exit
```

Configuration required on Clearpass for Guest Authentication

ClearPass Policy Manager Configuration

Adding DMZ controllers

Navigate to **ClearPass Policy Manager>Configuration > Network > Devices**. Click **Add** in the top-right corner to add controllers to the list. Note that the MCs have been added in a cluster using an IP range of 10.127.93.11-12.

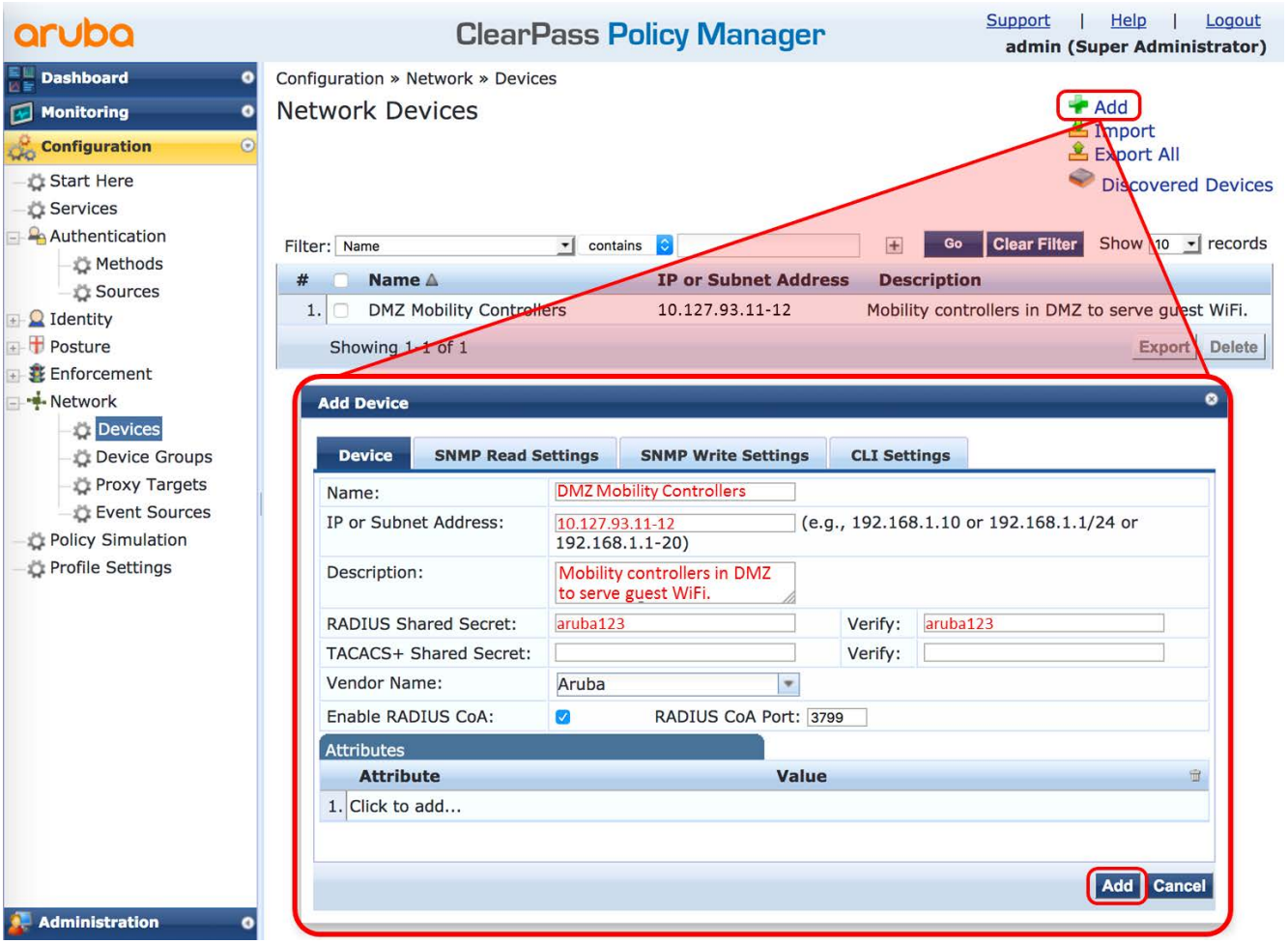


Figure 2 *Adding DMZ Controllers as Devices to ClearPass*

Adding Services for Guest Authentication

Navigate to **ClearPass Policy Manager>Configuration > Start Here**. Click **Guest Authentication with MAC Caching** to begin the wizard. Self-Registration will be added later when the Captive Portal is configured. Go through the wizard using the tabs, filling in the fields as follows. Everything else can be left blank or use the default value.

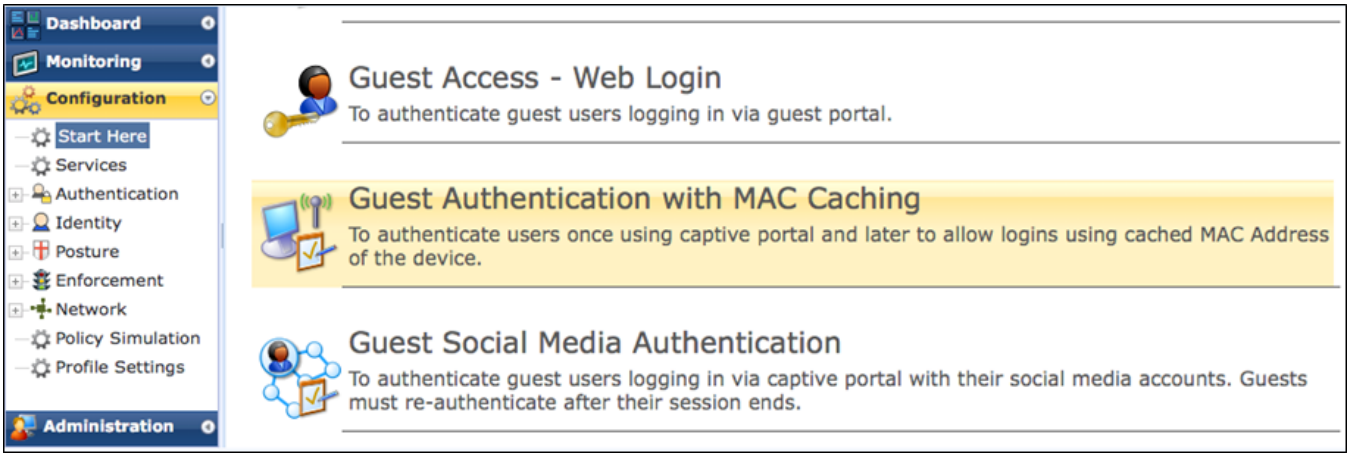


Figure 3 *Guest Authentication with MAC Caching*

General:

1. Navigate to the **General** tab
2. Enter guest-dmz as the **Name Prefix**
3. Click **Next**

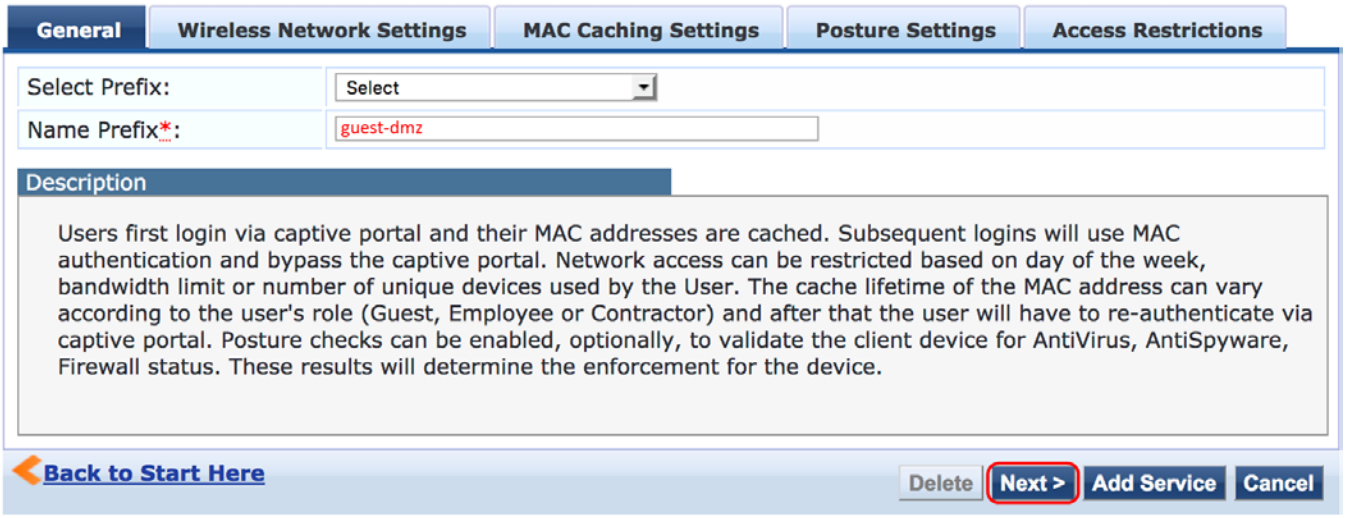


Figure 4 *General Tab*

Wireless Network Settings:

1. Navigate to the **Wireless Network Settings** tab
2. Enter the following details:
   - Wireless SSID: <TME-MobileFirst-Guest> (*This should match the SSID name on Campus side)*

- Select Wireless Controller: DMZ Mobility Controllers

3. Everything else can be left as default
4. Click **Next**

Figure 5 *Wireless Network Settings Tab*

MAC Caching Settings:

1. Navigate to the **MAC Caching Settings** tab
2. Enter *One Day* for **Cache duration for Guest**
3. Click **Next**

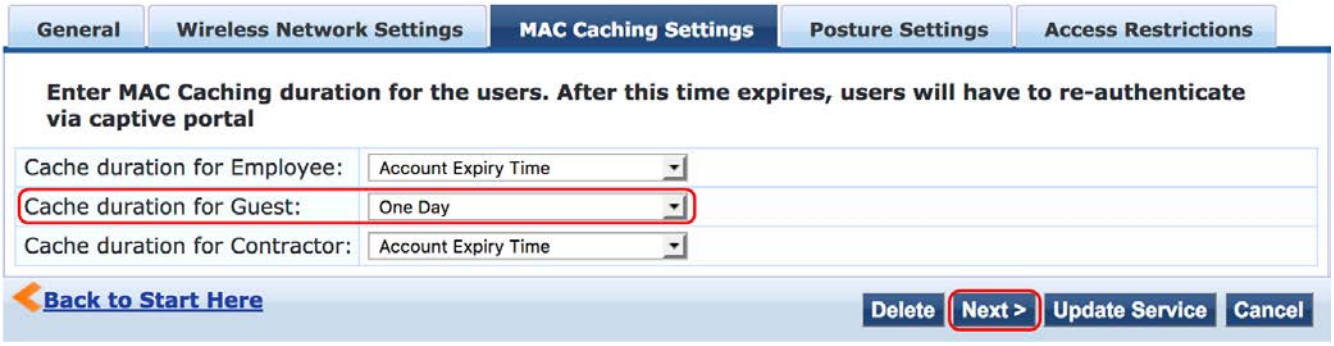


Figure 6 *MAC Caching Settings Tab*

Posture Settings:

1. Leave the **Posture Settings** tab blank
2. Click **Next**

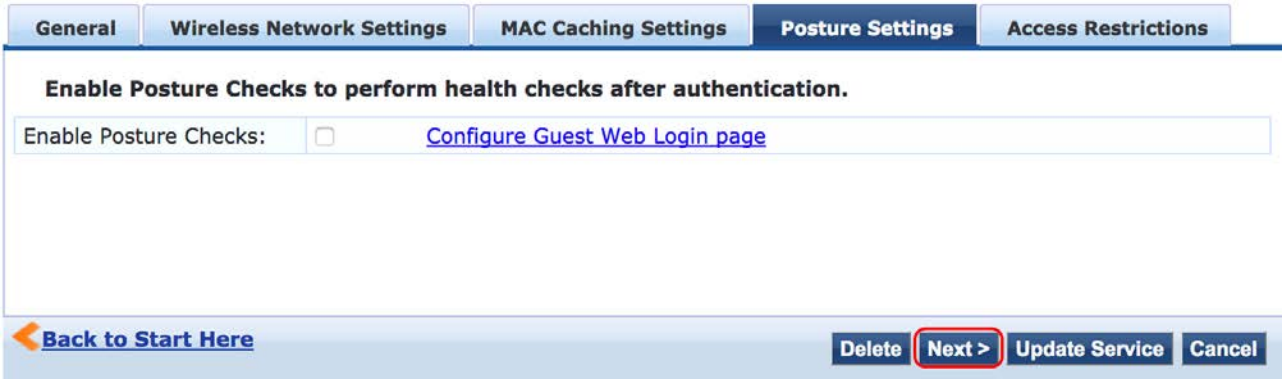


Figure 7 *Posture Settings Tab*

Access Restrictions:

1. Navigate to the **Access Restrictions** tab
2. Enter the following values:
   - Enforcement Type: Aruba Role Enforcement
   - Captive Portal Access: guest-dmz-logon
   - Maximum number of devices allowed per user: 3
   - Guest Access: guest-dmz
3. Everything else can be leave blank or in their default states.

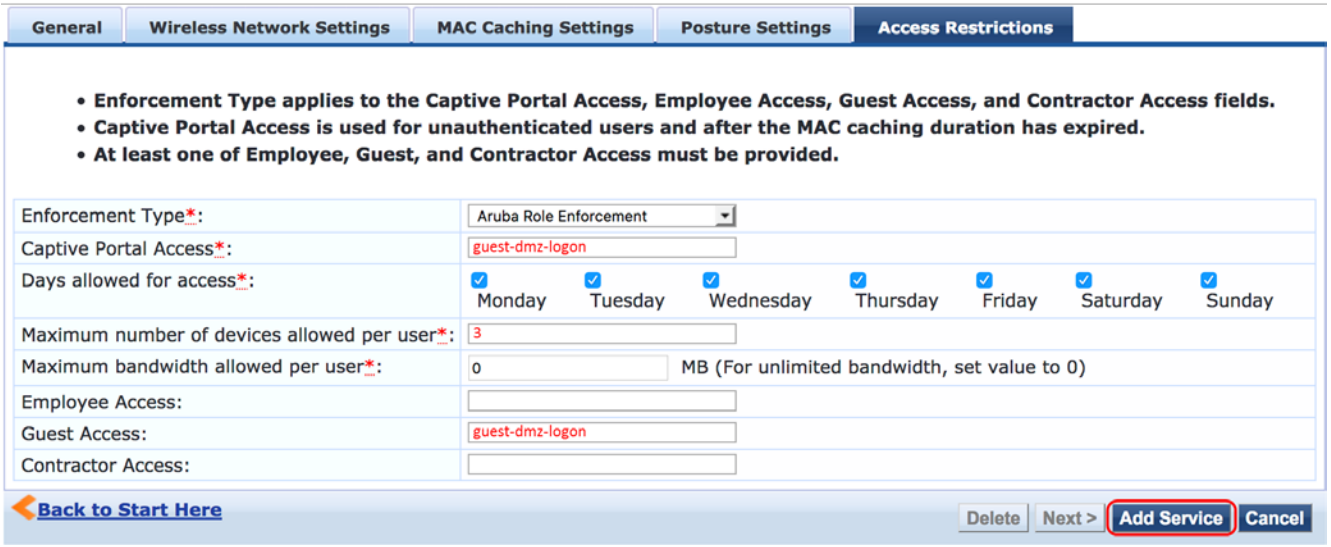


Figure 8 *Access Restrictions Tab*

Wizard Summary and Edit Services

ClearPass will notify that you have added a number of profiles, policies, and services that make up this solution. Notice also that *guest-dmz MAC Authentication* and *guest-dmz User Authentication with MAC Caching* were added to the list of services. It is important that MAC Authentication is

above User Authentication with MAC Caching. This order enables users to proceed to the self-registration captive portal page only if they fail MAC Authentication.

- **Added 8 Enforcement Profile(s)**
- **Added 2 Enforcement Policies**
- **Added 2 Role Mapping Policies**
- **Added 2 service(s)**

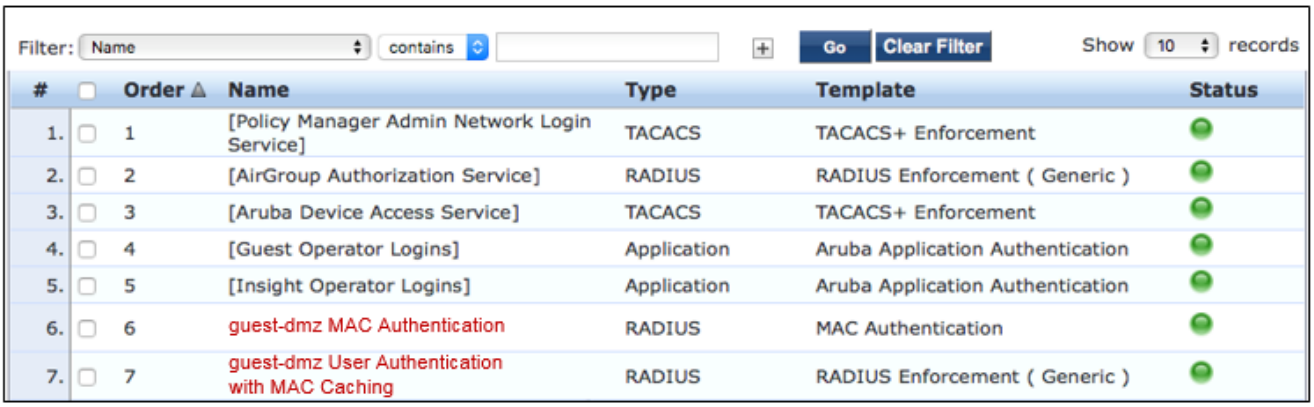


Figure 9 *Wizard Summary and Edit Services*

ClearPass Guest Configuration

Navigate to **ClearPass Guest>Configuration > Pages> Guest Self-Registrations**. Click **Create new self-registration page** in the top-right corner to add new self-registration page.

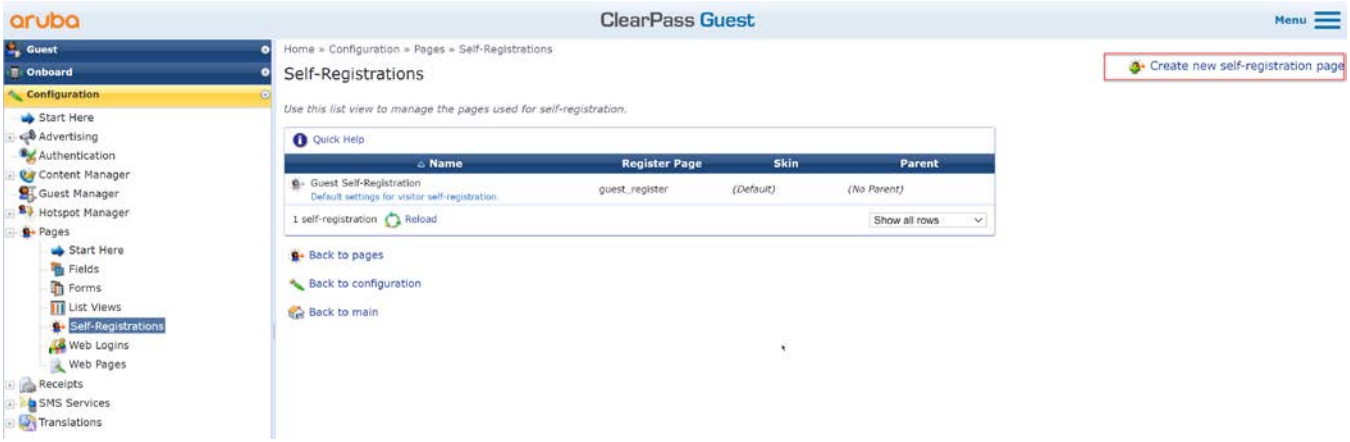


Figure 10 *Self-Registration Page Creation*

Please note the 'Register Page' value, since this will be used while setting the login-page value under captive portal on the DMZ MC. Eg: https://CPPM-IP/guest/**guest_registration**.php

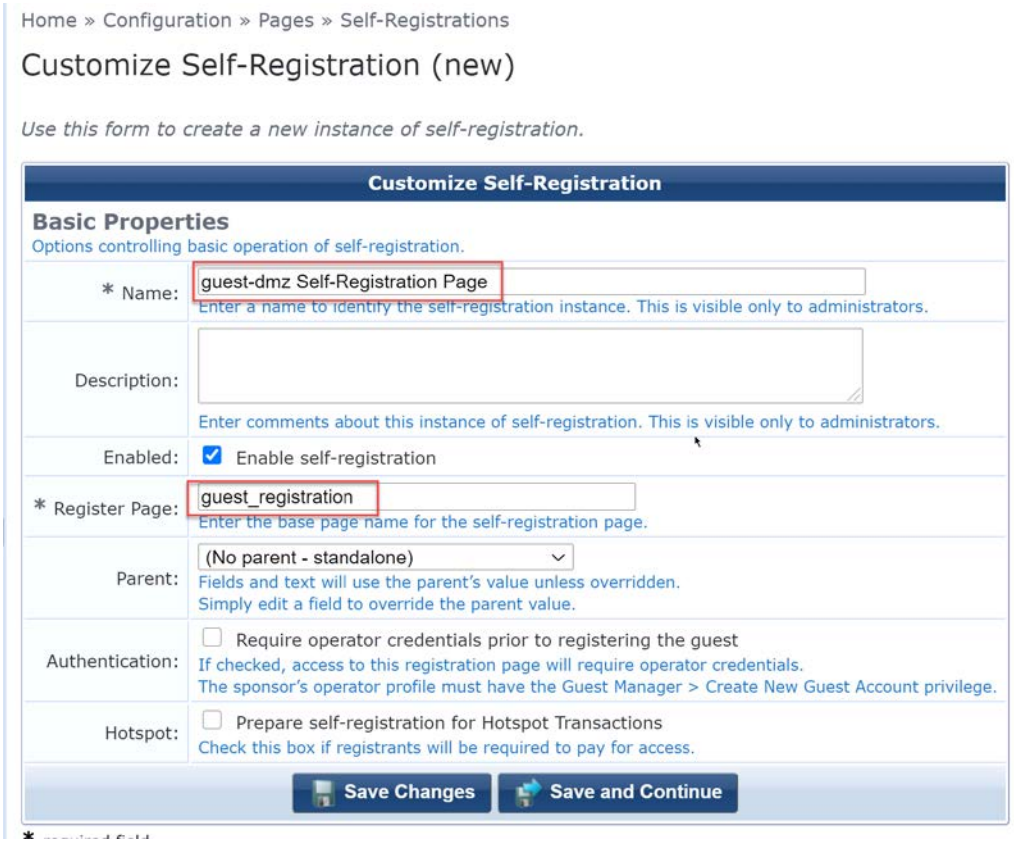


Figure 11 *Self-Registration Page Configuration*

Click **Save and Continue** till you reach the below page

Figure 12 *Self-Registration Page Configuration*

Click **Save and Continue** till you reach the below setting where you need to increase the 'Login Delay' to 2 seconds

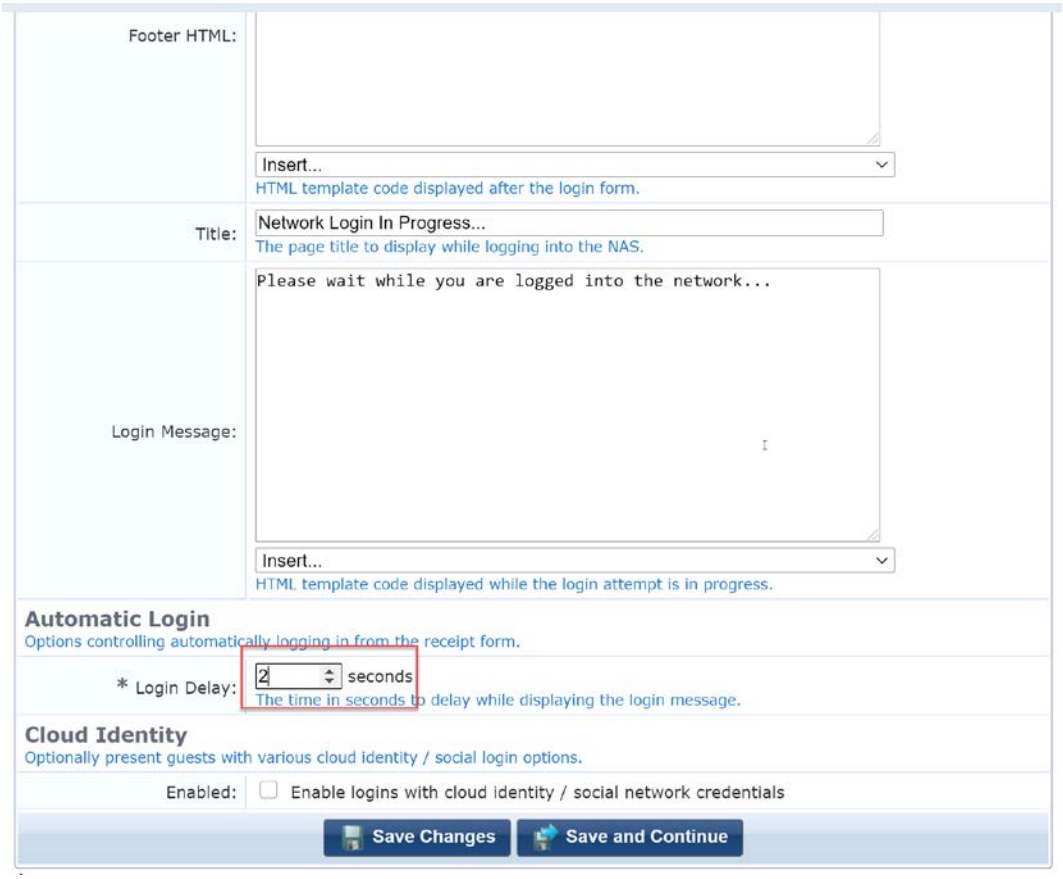


Figure 13 *Self-Registration Page Configuration*

Click **Save and Continue** and click **Save Changes** on the next page to finish this configuration.

Configuring L2 GRE

In the following two sections, the two options to configure L2 GRE tunnels from the controllers in cluster on Campus side to the DMZ controllers are discussed. Option 1 describes configuring tunnels from each individual Campus controller to the DMZ controllers and Option 2 describes configuring single tunnel from Campus controllers to the DMZ controllers. Refer to the details of these sections to learn about specific advantages of each as well as the ways to configure them.

Option 1: Configuring L2 GRE tunnels from each individual Campus MCs to DMZ MCs

In this scenario, L2 GRE tunnels need to be configured from each individual Campus MCs to DMZ MC VIP. This is the recommended design practice. This would mean that if there are 4 MCs in cluster at Campus side, there will be a total of 4 tunnels from each MC at Campus to DMZ MC VIP. From configuration standpoint: 1 tunnel each from individual MCs on Campus side to DMZ MC VIP and 4 tunnels each on both DMZ MCs from DMZ MC VIP to each Campus MCs.

Assumptions

- Campus MCs may or may not be configured to be in cluster.
- VRRP IP with L2 redundancy may or may not exist between the Campus MCs that are in the same L2 broadcast domain.
- DMZ MCs are standalone MCs which are configured together with a VRRP IP in L2 redundancy, if there is more than one MC.

Configuration

MC-IP used in the below sections are the controller-IP addresses of the individual controllers and DMZ-MC-VIP is the virtual IP which is configured to be in the same subnet of controller-IP addresses of individual controllers.

Campus side configuration

Configure L2 GRE tunnel on Campus MCs with DMZ MCs

```
(mcr01) [mc01] (config) #interface tunnel <1>
(mcr01) [mc01] (config-submode)#tunnel mode gre 1
(mcr01) [mc01] (config-submode)#tunnel source <MC1-IP>
(mcr01) [mc01] (config-submode)#tunnel destination <DMZ-MC-VIP>
(mcr01) [mc01] (config-submode)#tunnel keepalive
(mcr01) [mc01] (config-submode)#trusted
(mcr01) [mc01] (config-submode)#tunnel vlan 999  (This commands triggers the tunneling of traffic on vlan 999)
(mcr01) [mc01] (config-submode)#write memory
```

```
(mcr01) [mc02] (config) #interface tunnel <2>
(mcr01) [mc02] (config-submode)#tunnel mode gre 1
(mcr01) [mc02] (config-submode)#tunnel source <MC2-IP>
(mcr01) [mc02] (config-submode)#tunnel destination <DMZ-MC-VIP>
(mcr01) [mc02] (config-submode)#tunnel keepalive
(mcr01) [mc02] (config-submode)#trusted
(mcr01) [mc02] (config-submode)#tunnel vlan 999
(mcr01) [mc02] (config-submode)#write memory
```

Same configuration for MC 3 and 4

Check the status of the tunnels using: #`show interface tunnel`.

DMZ side configuration

```
(mc-dmz01) (config) #interface tunnel <1>
(mc-dmz01) (config-submode)#tunnel mode gre 1
(mc-dmz01) (config-submode)#tunnel source <DMZ-MC-VIP>
(mc-dmz01) (config-submode)#tunnel destination <MC1-IP>
(mc-dmz01) (config-submode)#tunnel keepalive
(mc-dmz01) (config-submode)#no inter-tunnel-flooding
(mc-dmz01) (config-submode)#tunnel vlan 999          (This commands triggers the tunneling of traffic on vlan 999)
(mc-dmz01) (config-submode)#write memory
```

```
(mc-dmz01) (config) #interface tunnel <2>
(mc-dmz01) (config-submode)#tunnel mode gre 1
(mc-dmz01) (config-submode)#tunnel source <DMZ-MC-VIP>
(mc-dmz01) (config-submode)#tunnel destination <MC2-IP>
(mc-dmz01) (config-submode)#tunnel keepalive
(mc-dmz01) (config-submode)#no inter-tunnel-flooding
(mc-dmz01) (config-submode)#tunnel vlan 999
(mc-dmz01) (config-submode)#write memory
```

Similar configuration for tunnel 3 and 4. Also, same set of config on other MC in the DMZ since this is device level config and cannot be done at higher node.

Check the status of the tunnels using: #`show interface tunnel`.

Option 2: Configuring a single L2 GRE tunnel from the VIP of Campus MCs to DMZ MCs

The use case described in Scenario 1 is recommended by Aruba. But if there is a need where the IT admins do not want to configure multiple individual tunnels from each Campus MC and instead just have 1 single tunnel from multiple Campus MCs, then configuration described in this second scenario can be used.

There is one fundamental issue which would arise in this case. When L2 redundancy is configured between the MCs in a cluster, one 'Master' MC is auto assigned by the system which will hold the VIP. Now if a client connects to an AP which is terminated on some other MC in the cluster, the return L2 GRE traffic will be dropped since the GRE tunnel is terminated on the VIP which is currently held by another MC.

To resolve this issue, the Guest VLAN needs to be configured on the uplink switch of the MCs. This way the traffic incoming from the DMZ will first reach the MC which holds the VIP through the tunnel, it will be then sent to its uplink switch since the intended destination for that traffic is the other MC. Once this reaches the uplink switch, it will then be forwarded to the correct MC.

Assumptions

- Campus MCs may or may not be configured to be in cluster.
- VRRP IP with L2 redundancy exists between the Campus MCs that are in the same L2 broadcast domain.
- DMZ MCs are standalone MCs which are configured together with VRRP IP with L2 redundancy, if there is more than one MC.
- Admin is ready to configure Guest VLAN on the uplink switch of the MCs

Configuration

MC-VIP and DMZ-MC-VIP used in the below sections are the virtual IP addresses which are configured to be in the same subnet of controller-IP addresses of individual controllers.

Campus side configuration

```
(mcr01) [mc01] (config) #interface tunnel <1>
(mcr01) [mc01] (config-submode)#tunnel mode gre 1
(mcr01) [mc01] (config-submode)#tunnel source <MC-VIP>
(mcr01) [mc01] (config-submode)#tunnel destination <DMZ-MC-VIP>
(mcr01) [mc01] (config-submode)#tunnel keepalive
(mcr01) [mc01] (config-submode)#trusted
(mcr01) [mc01] (config-submode)#no inter-tunnel-flooding
(mcr01) [mc01] (config-submode)#tunnel vlan 999            (This commands triggers the tunneling of traffic on vlan 999)
(mcr01) [mc01] (config-submode)#write memory
```

```
(mcr01) [mc02] (config) #interface tunnel <2>
(mcr01) [mc02] (config-submode)#tunnel mode gre 1
(mcr01) [mc02] (config-submode)#tunnel source <MC-VIP>
(mcr01) [mc02] (config-submode)#tunnel destination <DMZ-MC-VIP>
(mcr01) [mc02] (config-submode)#tunnel keepalive
(mcr01) [mc02] (config-submode)#trusted
(mcr01) [mc02] (config-submode)#no inter-tunnel-flooding
(mcr01) [mc02] (config-submode)#tunnel vlan 999
(mcr01) [mc02] (config-submode)#write memory
```

Same configuration for MC 3 and 4

Check the status of the tunnels using: #`show interface tunnel`.

Create Guest VLAN on the uplink switch of the MCs

```
SW-CORE-STACK #conf t
SW-CORE-STACK(config) #vlan 999
SW-CORE-STACK(vlan-999) #ip address 192.168.1.5 255.255.255.0
SW-CORE-STACK(vlan-999) #save
```

DMZ side configuration

```
(mc-dmz01)(config) #interface tunnel <1>
(mc-dmz01)(config-submode)#tunnel mode gre 1
(mc-dmz01)(config-submode)#tunnel source <DMZ-MC-VIP>
(mc-dmz01)(config-submode)#tunnel destination <MC-VIP>
(mc-dmz01)(config-submode)#tunnel keepalive
(mc-dmz01)(config-submode)#no inter-tunnel-flooding
(mc-dmz01)(config-submode)#tunnel vlan 999          (This commands triggers the tunneling of traffic on vlan 999)
(mc-dmz01)(config-submode)#write memory
```

Same configuration on the other MC in the DMZ.

Check the status of the tunnels using: #`show interface tunnel`.