Guest access solution with IAP’s GRE tunnels with webpage hosted on DMZ controller

Version: 0.1

Date: 5 April 2016

Authors: Vishal Mann

Contributors: Naveen Manjunath

# Introduction

GRE requires L3 connectivity without a NAT in place. It is typically deployed in scenarios where there is a WAN connectivity between the IAP and controller.

There is no known limit to GRE tunnels that can be terminated on the controller, unlike IPSec VPN tunnels that get terminated on controller.

However the disadvantage is security, as traffic encapsulated in GRE tunnel can easily deciphered, leaving only underlying security as the last frontier. On the other hand IPSec VPN tunnel are impossible to decrypt, and are standard security implementations.

It is pretty common for guests to be fully-tunneled via a Centralized layer 2 deployment. Typical use cases are where they want to isolate guest traffic on a separate CL2 VLAN and get everything to pass through their DMZ for regulatory reasons.

# Topology



# Flow



# Controller configuration & verification

1. Allow controller to accept IAP GRE tunnels.

whitelist-db rap add mac-address 94:b4:0f:cd:cf:dc ap-group default

show whitelist-db rap

Else following log will come up:

show log errorlog 10

Dec 14 02:04:49 authmgr[3820]: <522275> <ERRS> |authmgr| User Authentication failed. username=94:b4:0f:cd:cf:dc userip=192.168.3.101 usermac=94:b4:0f:cd:cf:dc servername=Internal serverip=192.168.2.5 apname=N/A bssid=00:00:00:00:00:00

Dec 14 02:04:49 localdb[3825]: <133006> <ERRS> |localdb| User 94:b4:0f:cd:cf:dc Failed Authentication

1. Add all the macaddresses you have to controller whitelist database, because any IAP upon failover can create tunnel, and thus needs to be whitelisted, also in case of per IAP GRE tunnel, each IAP creates the tunnel. You can use activate credentials to get all the IAP’s whitelisted easily.

CPPM can also be integrated with Activate for RAP/IAP Whitelisting: https://arubapedia.arubanetworks.com/arubapedia/index.php/RADIUS\_based\_Whitelist\_using\_CPPM\_ and\_Activate\_for\_IAP-VPN

1. Trust the branches you want the controller to create tunnel with

iap trusted-branch-db allow-all

show iap trusted-branch-db

Else following log will come up:

show log errorlog 10

Dec 14 02:05:20 IAP manager Process[3953]: <342001> <ERRS> |IAP manager Pro| !!! Not a trusted branch - '94b40fcdcfdc';remove this entry from white-list !!!

1. Create a pool to be used as inner IP for the tunnel

ip local pool "rapng" 172.16.1.100 172.16.1.200

(master) #show vpdn l2tp local pool

IP addresses used in pool rapng

172.16.1.101

Total:-

1 IPs used - 100 IPs free - 101 IPs configured

IP pool allocations / de-allocations - L2TP: 0/0 IKE: 2/2

(master) #show vpdn l2tp configuration

Enabled

Hello timeout: 60 seconds

DNS primary server: 0.0.0.0

DNS secondary server: 0.0.0.0

WINS primary server: 0.0.0.0

WINS secondary server: 0.0.0.0

PPP client authentication methods:

PAP

IP LOCAL POOLS:

rapng: 172.16.1.100 - 172.16.1.200

1. Verify on the controller if the tunnel has come up

(master) #show iap table

Trusted Branch Validation: Disabled

IAP Branch Table

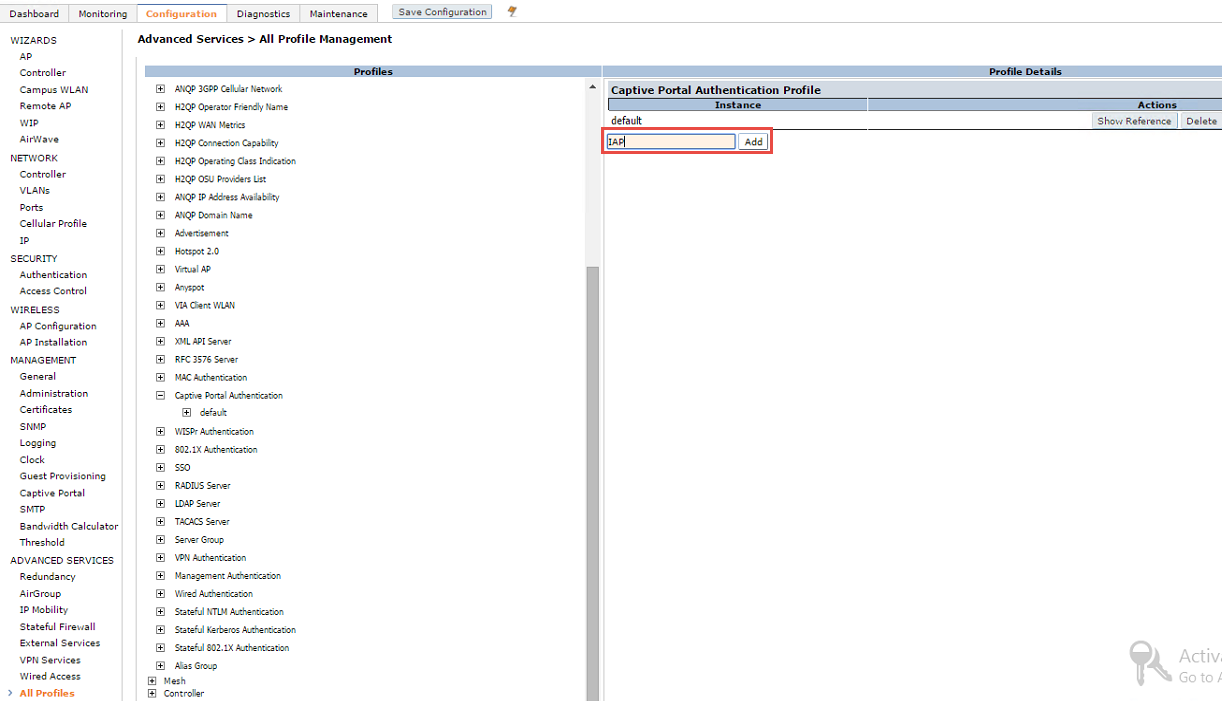
----------------

Name VC MAC Address Status Inner IP Assigned Subnet Assigned Vlan

---- -------------- ------ -------- --------------- -------------

instant-C0:62:7C 18:64:72:c0:62:7c UP 172.16.1.101 50

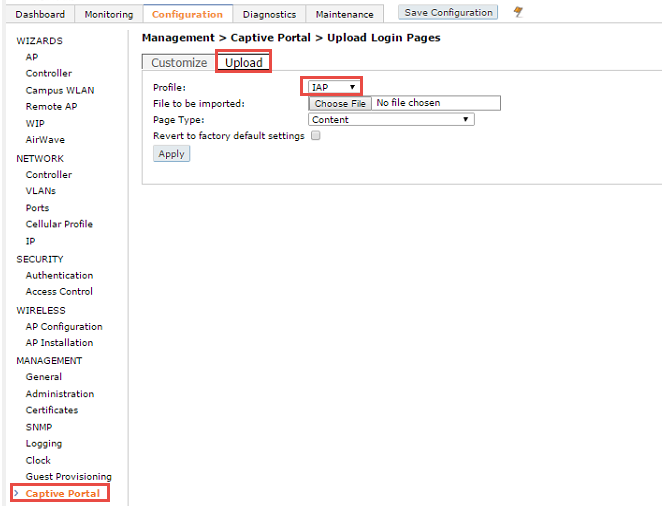
1. Extend a VLAN from connected switch to controller, to the controller, to be used for CL2 VLAN, by adding it to the trunk to controller and creating a default gateway on the connected switch. Ensure appropriate routing for that VLAN to DHCP server and CPPM is in place.
2. Create a new captive portal authentication profile.

Controller GUI> Configuration> Advanced services> All profiles> Captive portal authentication

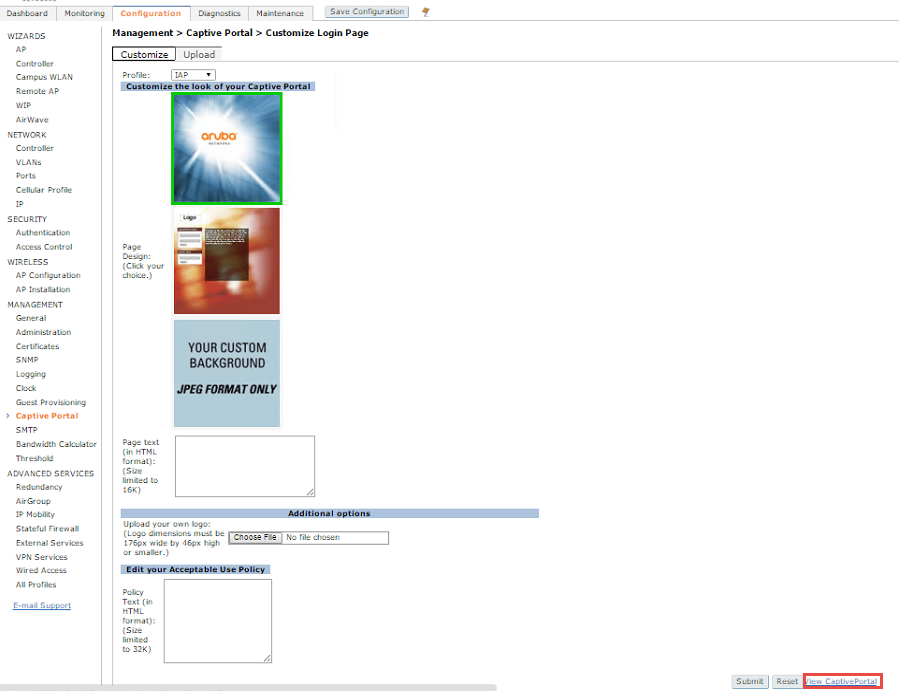
1. Upload custom web page

Controller GUI> Configuration> Management> Captive Portal> Upload

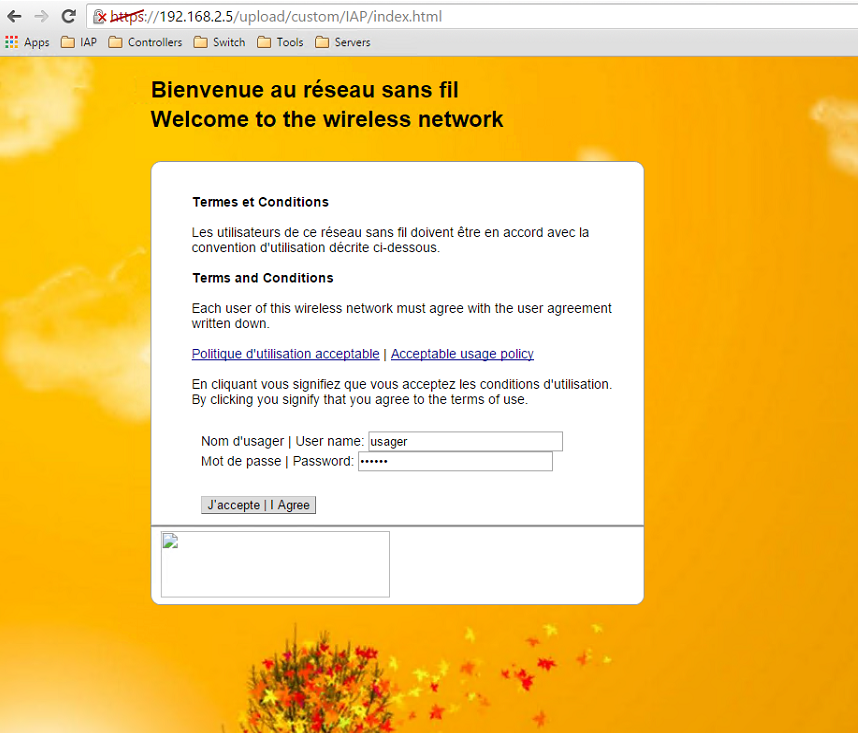
From the attached folder upload all seven files to controller, under IAP profile created above. Choose all the files other than “index.html” as content. Upload “index.html” as CP login (top-level). When you hit apply, look for the message, “Upload Successfully Completed”.



1. Verify uploaded webpage, Controller GUI> Configuration> Management> Captive Portal> Customize

Choose profile as created above, in this case “IAP”, and hit “view captive portal”.

A separate tab will show



1. What is special in the webpages?

The web pages uploaded & served by controller, to the end client, have a mechanism to provide username and password entered in the web login page, to IAP, via a POST request.

Opposite to a GET request, POST request, the POSTrequest method requests that a web server accepts and stores the data enclosed in the body of the request message. It is often used when uploading a file or submitting a completed web form. As part of a POST request, an arbitrary amount of data of any type can be sent to the server in the body of the request message.

If you open the index.html in notepad, you will see the code

<form method=POST action="http://securelogin.arubanetworks.com/cgi-bin/login">

<span class="bodytext">

Nom d'usager | User name: <input id="user" name="user" value="usager" type="text" size="25" class="text" accesskey="u" /><br>

Mot de passe | Password: <input id="password" name="password" value="usager" type="password" size="25" class="text" accesskey="p" /><br><br>

The above code is responsible to POST the username password field’s value to, securelogin.arubanetworks.com, via HTTPS. securelogin.arubanetworks.com is intercepted and hosted by the IAP itself.

Once the IAP has username and password obtained via the above method, it will authenticate them via the method defined on the SSID for authentication, Internal RADIUS or external RADIUS server.

1. Verify using:

(master) #show aaa authentication captive-portal IAP

Captive Portal Authentication Profile "IAP"

-------------------------------------------

Parameter Value

--------- -----

Default Role guest

Default Guest Role guest

Server Group default

Redirect Pause 10 sec

User Login Enabled

Guest Login Disabled

Logout popup window Enabled

Use HTTP for authentication Disabled

Logon wait minimum wait 5 sec

Logon wait maximum wait 10 sec

logon wait CPU utilization threshold 60 %

Max Authentication failures 0

Show FQDN Disabled

Authentication Protocol PAP

Login page /upload/custom/IAP/index.html

Welcome page /auth/welcome.html

Show Welcome Page Yes

Add switch IP address in the redirection URL Disabled

Adding user vlan in redirection URL Disabled

Add a controller interface in the redirection URL N/A

Allow only one active user session Disabled

White List N/A

Black List N/A

Show the acceptable use policy page Disabled

User idle timeout N/A

Redirect URL N/A

Bypass Apple Captive Network Assistant Disabled

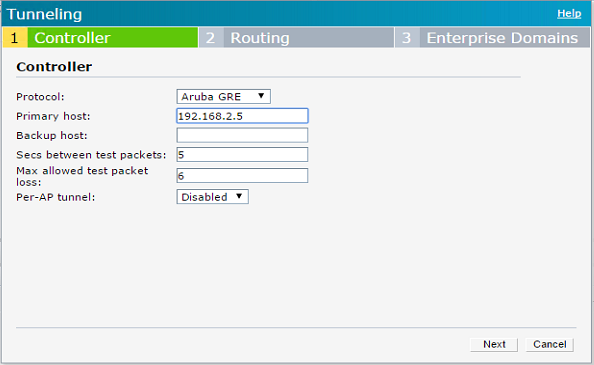
URL Hash Key N/A

# IAP configuration & verfication

1. Setup Aruba GRE tunnel.

Do not use Aruba GRE if the controller’s reachability from IAP is across a NAT. GRE requires L3 connectivity without a NAT in place between IAP and controller. It is typically deployed in scenarios where there is a WAN connectivity between the IAP and controller.

GUI

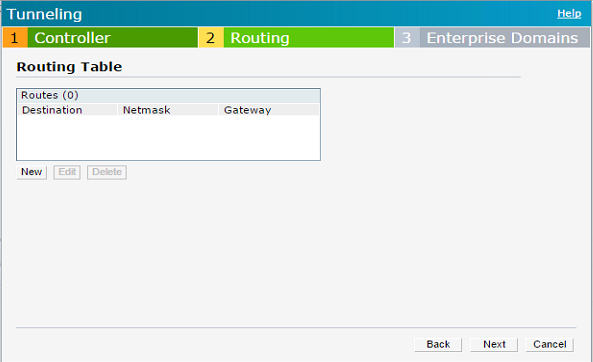


Choose protocol as Aruba GRE and provide controller’s L3 routable IP as primary host.

Per-AP GRE tunnel is an important concept, and would be covered in another document. But in a nutshell, if you disable this feature, then each slave has to tag its traffic with CL2 VLAN id on the SSID and bridge it to master IAP first, from master the traffic is GRE tunneled to controller.

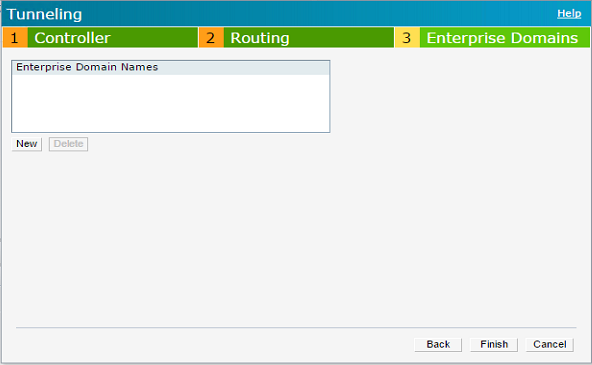
Disadvantage if not using per-AP tunnel, the switch where master and slaves are connected, have to be configured for the CL2 VLAN.

If you enable per-AP tunnel feature, then each slave creates a separate GRE tunnel to controller, and there is no need to configure the switch for the VLAN.



Routing profile decides for what traffic needs to be GRE tunneled to controller.

1. This setting is used for the WLAN only if split tunnel knob in CL2 DHCP profile is set to enabled.



Enterprise domain

By default all DNS requests for VPN tunneled VLANs are proxied to the DNS server of IAP. The domain names defined here are treated outside the above rule and DNS requests are sent to actual DNS server of the client.

CLI configuration

vpn primary 192.168.2.5

vpn gre-outside

1. Verify the tunnel is up, by

Show vpn status

Show vpn config

Show vpn tunnels

18:64:72:c0:62:7c# show vpn config

Concentrator

------------

Type Value

---- -----

VPN Primary Server 192.168.2.5

VPN Backup Server

VPN Preemption disable

VPN Fast Failover disable

VPN Hold Time 600

VPN Monitor Pkt Send Freq 5

VPN Monitor Pkt Lost Cnt 6

VPN Ikepsk 5fc76ef7710b3b9fa4c6e7e227d63315

VPN Username

VPN Password bb75df9b57213e14832b569f9b39084c

GRE outside vpn enable

GRE Server

GRE IP Address 0.0.0.0

GRE Type 1

GRE Per AP Tunnel disable

Reconnect User On Failover disable

Reconnect Time On Failover 60

Routing Table

-------------

Destination Netmask Gateway Type

----------- ------- ------- ----

18:64:72:c0:62:7c# show vpn status

profile name:default

--------------------------------------------------

current using tunnel :primary tunnel

current tunnel using time :2 hours 52 minutes 46 seconds

ipsec is preempt status :disable

ipsec is fast failover status :disable

ipsec hold on period :600s

ipsec tunnel monitor frequency (seconds/packet) :5

ipsec tunnel monitor timeout by lost packet cnt :6

ipsec primary tunnel crypto type :Cert

ipsec primary tunnel peer address :192.168.2.5

ipsec primary tunnel peer tunnel ip :192.168.2.5

ipsec primary tunnel ap tunnel ip :172.16.1.101

ipsec primary tunnel using interface :tun0

ipsec primary tunnel using MTU :1230

ipsec primary tunnel current sm status :Up

ipsec primary tunnel tunnel status :Up

ipsec primary tunnel tunnel retry times :34

ipsec primary tunnel tunnel uptime :2 hours 52 minutes 46 seconds

ipsec backup tunnel crypto type :Cert

ipsec backup tunnel peer address :N/A

ipsec backup tunnel peer tunnel ip :N/A

ipsec backup tunnel ap tunnel ip :N/A

ipsec backup tunnel using interface :N/A

ipsec backup tunnel using MTU :N/A

ipsec backup tunnel current sm status :Init

ipsec backup tunnel tunnel status :Down

ipsec backup tunnel tunnel retry times :0

ipsec backup tunnel tunnel uptime :0

18:64:72:c0:62:7c# show vpn tunnels

Tunnel Flags: M = Master IAP; S = Slave IAP; Primary = Primary Tunnel

B = Backup Tunnel; R = Registered

Tunnel Info for peer address 192.168.2.5

------------------------------------------

Type Value

---- -----

Source IP 172.16.1.101

Destination IP 192.168.2.5

End IP 192.168.2.5

Default GW 0.0.0.0

Use count 0

Ifindex 12

Ifname tun0

Flags MPR

Retry count for Register Request 0

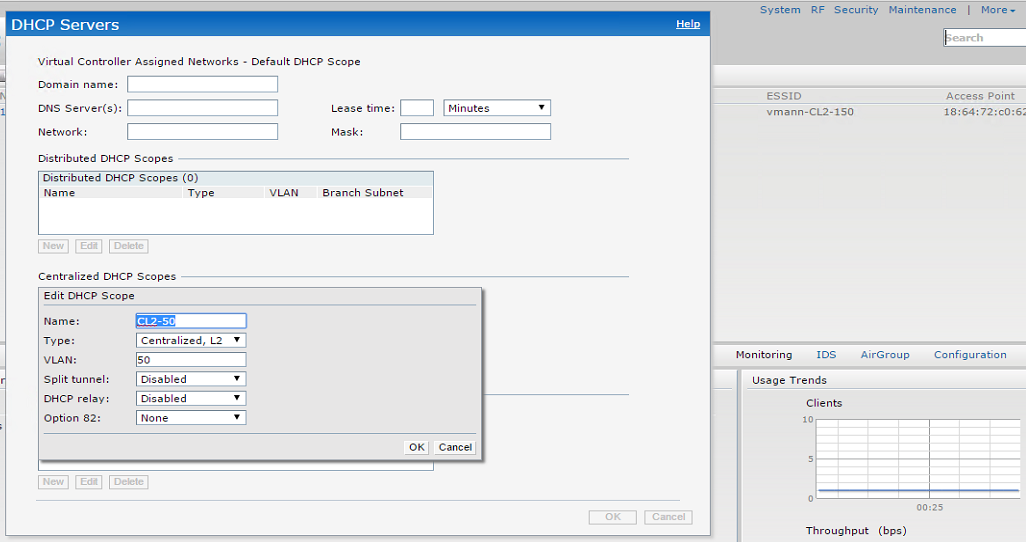
For DHCP Profile CL2-50

Retry count for Vlan Add Request 0

Old Subnet Status Normal

Existing Subnet Status Registered

1. Create a DHCP server profile CL2



Notice that I have disabled split tunnel and that will cause all the traffic to go via the GRE tunnel.

ip dhcp CL2-50

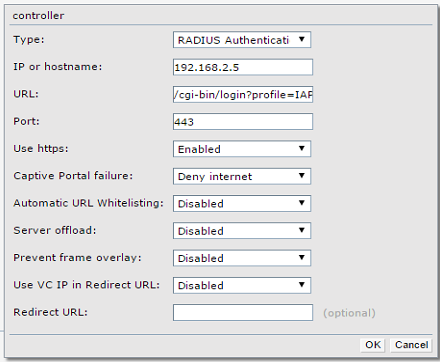
server-type Centralized,L2

server-vlan 50

disable-split-tunnel

1. Create an external captive portal profile

IAP GUI> Security> External Captive Portal> New



1. Type must be chosen as RADIUS authentication.

IP address field in this case will be where webpage is hosted, i.e. controller’s IP.

1. This solution does not provide inter datacenter redundancy, but does provide intra datacenter redundancy. Note that you can only provide one IP address here. This IP address can be of one controller or two controllers in VRRP with in a datacenter.

URL field is /cgi-bin/login?profile=<profile name>

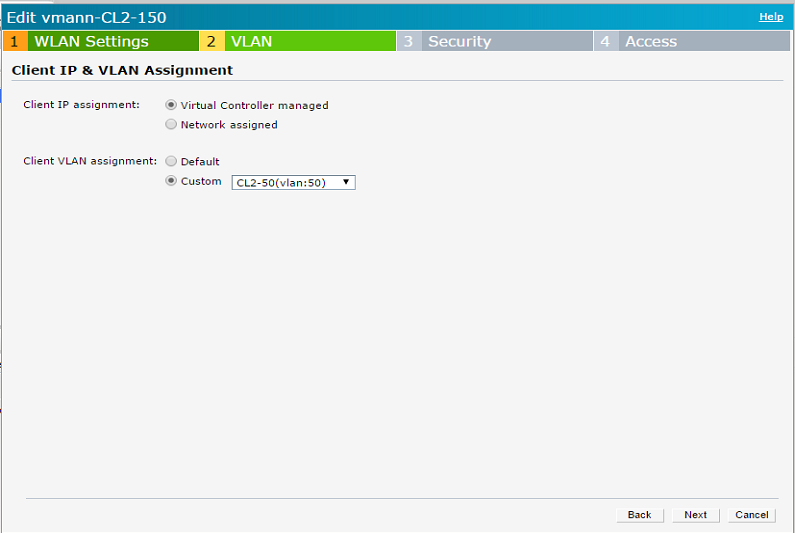
In the above example it is:

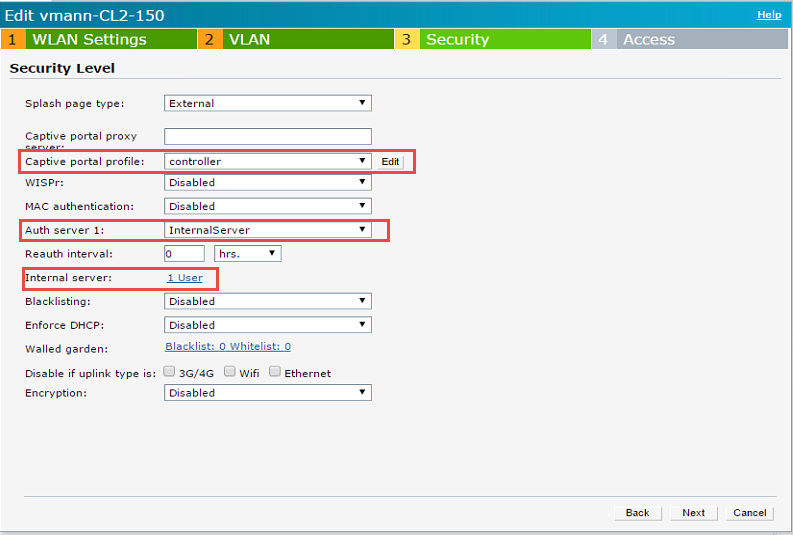
/cgi-bin/login?profile=IAP

1. Pay very close attention to the last variable, profile name. In this case it is the new profile I defined on the controller, named as “IAP” will be used. It will differ based on the profile you use on the controller.

Use port as 443 and HTTPS as enabled. This causes the username and password to travel inside a tunnel. Leave rest of the fields as default. In the last field of Redirect URL, use a URL if you want to redirect the client after a successful authentication. By default the clients are redirected to www.arubanetworks.com.

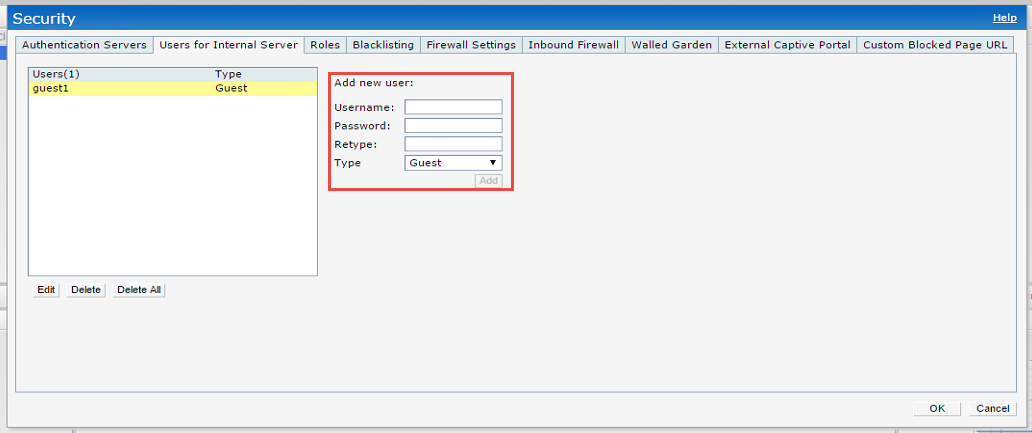
Create a guest SSID, and for VLAN settings map it to the DHCP server profile created and the external captive portal profile created.





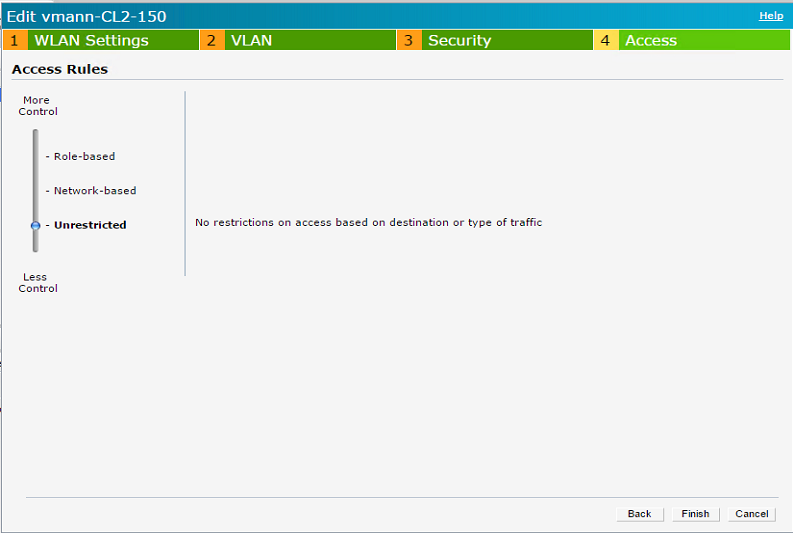
Notice that the captive portal profile is chosen as the profile I created previously, named as “controller”.

For authentication, IAP’s internal database is used, I have created one user in the internal database.



IAP GUI> Security> users for Internal Server. Choose type as “Guest”.

Leave the access settings on SSID as “Unrestricted”.



Resulting CLI configuration:

wlan ssid-profile vmann-CL2-150

enable

index 0

type guest

essid vmann-CL2-150

opmode opensystem

max-authentication-failures 0

vlan 50

auth-server InternalServer

rf-band 2.4

captive-portal external profile controller

dtim-period 1

broadcast-filter arp

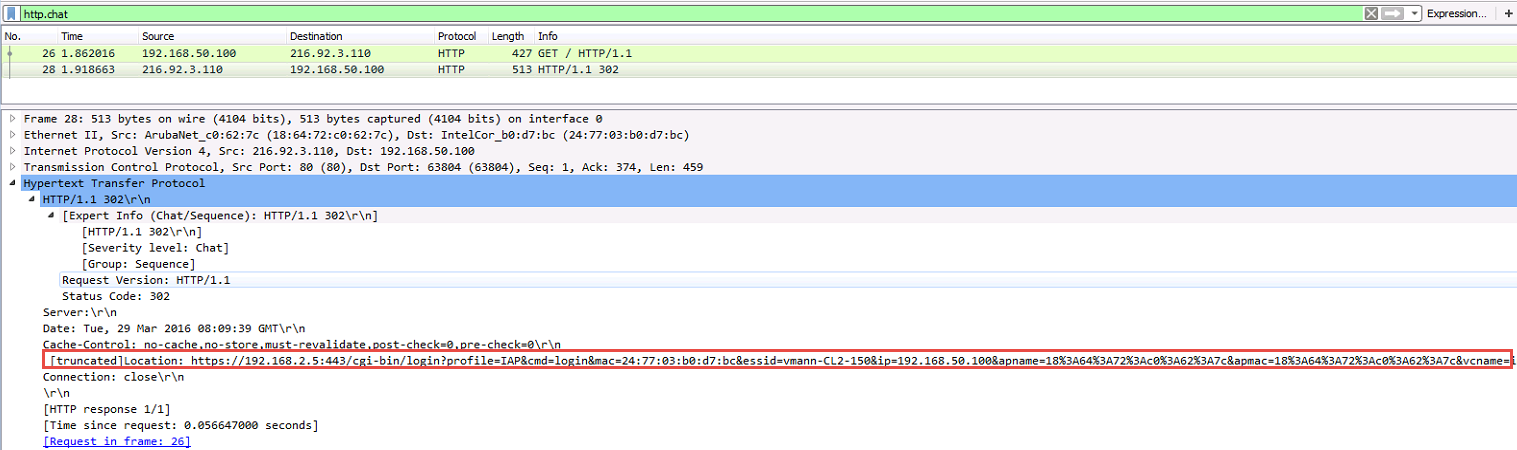
dmo-channel-utilization-threshold 90

local-probe-req-thresh 0

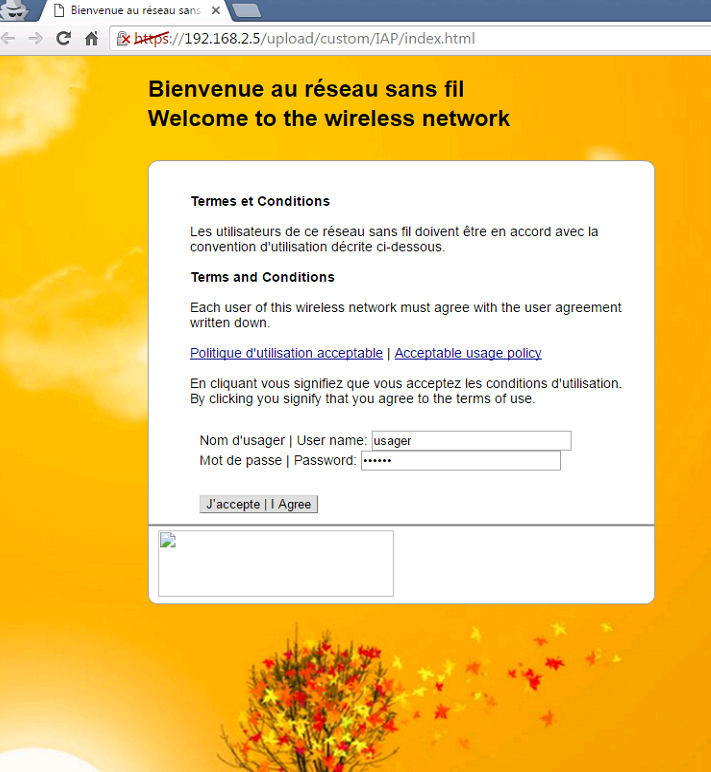
max-clients-threshold 64

Now connect the client to the created SSID, making sure it has only wireless connectivity.

DNS should work as a prerequisite. As a result whatever the homepage the client is trying to access will be first resolved by DNS server and then the client tries to set up a HTTP session with the end server, which is redirected by IAP to the controller’s login page defined above. Following is a screen shot of HTTP 302 response redirecting the client 192.168.50.100:



As a result the login page hosted on controller will be presented to the end client:



From here onwards the controller is out of picture. It has done its job of providing the webpage to the end client.

Check the output of show clients on the IAP to check the role client is in:

18:64:72:c0:62:7c# show clients

Client List

-----------

Name IP Address MAC Address OS ESSID Access Point Channel Type Role Signal Speed (mbps)

---- ---------- ----------- -- ----- ------------ ------- ---- ---- ------ ------------

CTO-POCLabAdmin 192.168.50.100 24:77:03:b0:d7:bc Win 7 vmann-CL2-150 18:64:72:c0:62:7c 6 GN External CP 70(good) 195(good)

Number of Clients :1

Info timestamp :33825

Check the ACL mapped to client:

18:64:72:c0:62:7c# show datapath user

Datapath User Table Entries

---------------------------

Flags: P - Permanent, W - WEP, T- TKIP, A - AESCCM

R - ProxyARP to User, N - VPN, L - local, I - Intercept, D - Deny local routing

FM(Forward Mode): S - Split, B - Bridge, N - N/A

IP MAC ACLs Contract Location Age Sessions Flags Vlan FM MediaSessCnt

--------------- ----------------- ------- --------- -------- ----- --------- ----- ---- -- ------------

192.168.50.100 24:77:03:B0:D7:BC 109/0 0/0 0 15 0/65535 50 B 0

Notice the client has role, “External CP”. Its an inbuilt role that allows access to the webpage server, DHCP and DNS we never defined that role. You do not have to configure it.

The ACL applied to client is 109. Lets see what is in the ACL:

18:64:72:c0:62:7c# show datapath acl 109

Datapath ACL 109 Entries

-----------------------

Flags: P - permit, L - log, E - established, M/e - MAC/etype filter

S - SNAT, D - DNAT, R - redirect, r - reverse redirect m - Mirror

I - Invert SA, i - Invert DA, H - high prio, O - set prio, C - Classify Media

A - Disable Scanning, B - black list, T - set TOS, t - time based, o - tunnel only

K - App Throttle, s - Domain SA, d - Domain DA, 4 - IPv4, 6 - IPv6

----------------------------------------------------------------

1: any any 17 0-65535 8209-8211 P4

2: any 172.31.98.1 255.255.255.255 6 0-65535 80-80 172.31.98.2 172.31.98.1 80 PSD4 hits 1

3: any 172.31.98.1 255.255.255.255 6 0-65535 443-443 172.31.98.2 172.31.98.1 443 PSD4

**4: any 192.168.2.5 255.255.255.255 6 0-65535 80-80 P4 hits 3**

**5: any 192.168.2.5 255.255.255.255 6 0-65535 443-443 P4 hits 50**

6: any any 6 0-65535 80-80 172.31.98.2 172.31.98.1 8080 PSD4 hits 6

7: any any 6 0-65535 8080-8080 172.31.98.2 172.31.98.1 8080 PSD4

8: any any 6 0-65535 443-443 172.31.98.2 172.31.98.1 4343 PSD4 hits 20

9: 172.31.98.0 255.255.254.0 172.31.98.0 255.255.254.0 17 0-65535 67-68 P4

10: 172.31.98.0 255.255.254.0 224.0.0.0 224.0.0.0 17 0-65535 67-68 P4

11: 172.31.98.0 255.255.254.0 any 17 0-65535 67-68 192.168.6.100 PS4

12: any any 17 0-65535 67-68 P4 hits 7

13: 172.31.98.0 255.255.254.0 172.31.98.0 255.255.254.0 17 0-65535 53-53 P4

14: 172.31.98.0 255.255.254.0 224.0.0.0 224.0.0.0 17 0-65535 53-53 P4

**15: 172.31.98.0 255.255.254.0 any 17 0-65535 53-53 192.168.6.100 PS4**

**16: any any 17 0-65535 53-53 P4 hits 141**

17: 172.31.98.0 255.255.254.0 172.31.98.0 255.255.254.0 6 0-65535 8081-8081 P4

18: 172.31.98.0 255.255.254.0 224.0.0.0 224.0.0.0 6 0-65535 8081-8081 P4

19: 172.31.98.0 255.255.254.0 any 6 0-65535 8081-8081 192.168.6.100 PS4

20: any any 6 0-65535 8081-8081 P4

21: 0x888e 0xffff any any Pe4

22: 0x0806 0xffff any any Pe4 hits 8

23: any any any e4 hits 13

24: any any any 4 hits 73

For details check:

show datapath acl-rule-detail 109

Now the username and password put on the webpage will be sent to IAP via a POST request.

IAP will authenticate the user via the internal username database or external RADIUS database if configured. The rules in routing profile will decide how IAP will reach out to the RADIUS server, via GRE tunnel or outside it.

18:64:72:c0:62:7c# show ap debug auth-trace-buf ?

<cr>

<mac> mac

Once authenticated, the client will move to the default role on the SSID and will be redirected to the URL configured in the external captive portal profile.

18:64:72:c0:62:7c# show clients

Client List

-----------

Name IP Address MAC Address OS ESSID Access Point Channel Type **Role** Signal Speed (mbps)

---- ---------- ----------- -- ----- ------------ ------- ---- ---- ------ ------------

guest1 192.168.50.100 24:77:03:b0:d7:bc Win 7 vmann-CL2-150 18:64:72:c0:62:7c 6 GN **vmann-CL2-150** 63(good) 195(good)

Number of Clients :1

Info timestamp :34595

## Trusted vs untrusted

GRE tunnels created via the above method are trusted on controller that means client entry will be in bridge table, but will not be assigned a user role. Hence the traffic does not pass via controller’s firewall. All the firewall policies are configured on IAP itself. And as you have seen in the above example the roles are present on IAP.

(master) #show datapath tunnel

Datapath Tunnel Table Entries

-----------------------------

Flags: E - Ether encap, I - Wi-Fi encap, R - Wired tunnel, F - IP fragment OK

W - WEP, K - TKIP, A - AESCCM, G - AESGCM, M - no mcast src filtering

S - Single encrypt, U - Untagged, X - Tunneled node, 1(cert-id) - 802.1X Term-PEAP

2(cert-id) - 802.1X Term-TLS, T - Trusted, L - No looping, d - Drop Bcast/Unknown Mcast,

D - Decrypt tunnel, a - Reduce ARP packets in the air, e - EAPOL only

C - Prohibit new calls, P - Permanent, m - Convert multicast

n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split tunnel

V - enforce user vlan(open clients only), x - Striping IP

H - Standby (HA-Lite), c - IP Compression, g - PAN GlobalProtect Tunnel

# Source Destination Prt Type MTU VLAN Acls BSSID Decaps Encaps Heartbeats Flags EncapKBytes DecapKBytes

------ -------------- -------------- --- ---- ---- ---- ----------------------- ----------------- ---------- ---------- ---------- ----- ------------- -----------

17 192.168.2.5 192.168.6.100 47 1 1200 0 0 0 2 0 0 00:00:00:00:00:00 59031 79580 0 TEFP

Notice the protocol 47, for the IP 192.168.6.100, that means it’s a GRE tunnel. One of the flags is T, which means the tunnel is trusted.

Even when a client is connected on the controller a role for the client entry will not exist. See in the below output, only the IAP itself is using a role in controller, via its actual IP and inner IP. There is no entry for the client connected to IAP.

(master) #show user-table

Users

-----

IP MAC Name Role Age(d:h:m) Auth VPN link AP name Roaming Essid/Bssid/Phy Profile Forward mode Type Host Name

---------- ------------ ------ ---- ---------- ---- -------- ------- ------- --------------- ------- ------------ ---- ---------

192.168.6.100 00:00:00:00:00:00 logon 00:03:55 VPN N/A tunnel

172.16.1.101 00:00:00:00:00:00 18:64:72:c0:62:7c default-vpn-role 00:03:47 VPN 192.168.6.100 N/A default-iap tunnel

User Entries: 2/2

Curr/Cum Alloc:2/5 Free:0/3 Dyn:2 AllocErr:0 FreeErr:0

192.168.6.100 is the IAP IP and 172.16.1.101 is the inner IP for IAP.

However the client entry will be in datapath bridge table

(master) #show datapath bridge table

Datapath Bridge Table Entries

-----------------------------

Flags: P - Permanent, D - Deny, R - Roamed Client, M - Mobile, X - Xsec, A - Auth, T - Trusted

MAC VLAN Assigned VLAN Destination Flags Age

----------------- ---- ------------- ----------- ------- ----

24:77:03:B0:D7:BC 50 50 tunnel 17 0

Now that you have understood the basics, then you can use ClearPass instead of local data base, as well.