1 Table of Contents

Table of Contents

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
07 Jul 2019	0.1	Ariya Parsamanesh	Initial creation

2 Client Isolation Feature

There are always cases where you need to ensure that the traffic between Wireless clients with in a subnet are not allowed. In the past using Instant APs (IAP), we could use Broadcast filter All (block Broadcasts and Unknown multicast. Except DHCP and ARP) and also enabling Deny inter user bridging feature that would provide client isolation only for the clients that were connected to the same IAP.

With the Instant 8.5 version we have this new feature Client Isolation, which enables you to disable all client-to-client traffic with in a subnet. For some use cases this feature can be used to improve the security of the network infrastructure and protects it against vulnerabilities. At this point Client Isolation can only be configured through the CLI.

This short tutorial will go through this feature and demonstrate it.

2.1 Things you need

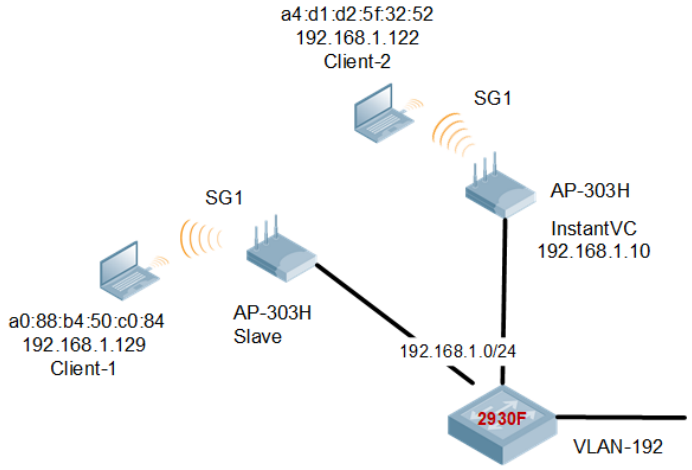
- Aruba Instant version 8.5.0.0 or later
- 2x IAPs
- A Layer three switch

3 Instant AP Configuration

Client isolation feature is supported through the CLI for now. The following is our topology.

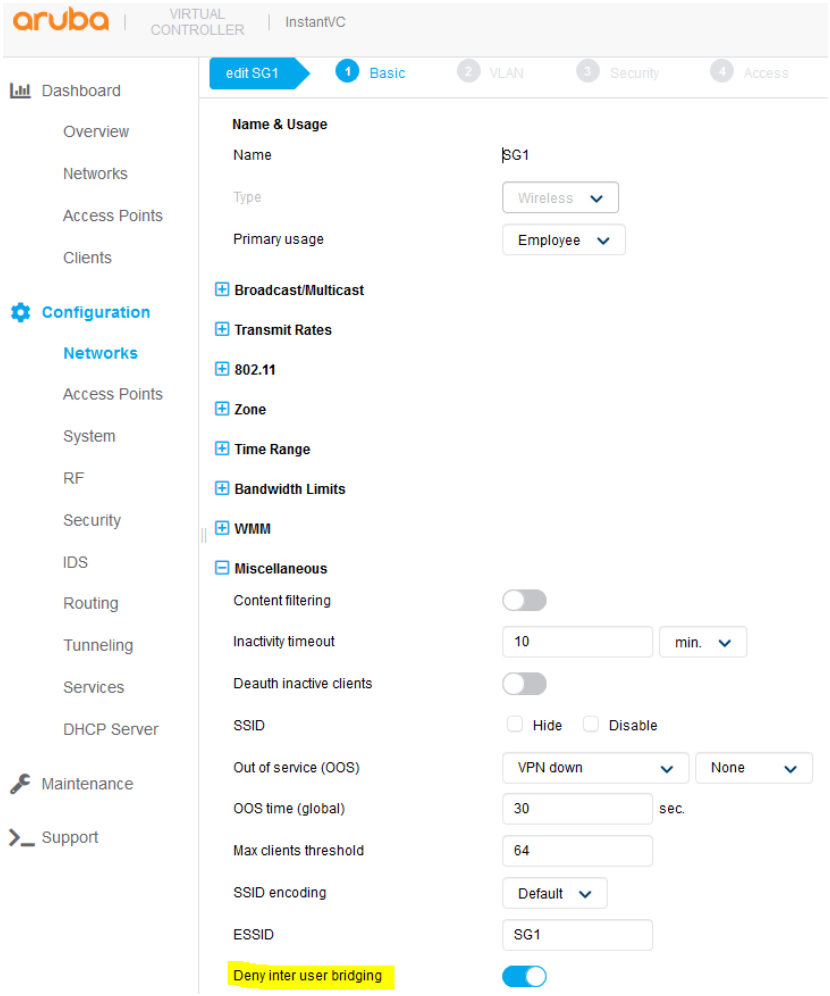
Previously we had a feature called “Deny inter user bridging” that would disable traffic between two clients connected to the same Instant AP on the same VLAN. You could enable it at the SSID level or at the global level.

So using “Deny inter user bridging” on SG1 WLAN, Client-1 could still ping Client 2



3.1 Deny Inter User Bridging Configuration

Here we have configured “Deny inter user bridging” for SG1 SSID.



Here we see that the Clients 1 and 2 are on different IAPs.

```
BLDG-A-ATV1# sh clients

Client List
-----------
Name             IP Address     MAC Address        OS       ESSID  Access Point       Channel  Type
Role           IPv6 Address                            Signal    Speed (mbps)
----             ----------     -----------        --       -----  ------------       -------  ----

AriyaP           192.168.1.129  a0:88:b4:50:c0:84  Win 10   SG1    20:4c:03:23:a7:98  36+      AN
SG1            fd14:5f94:8156:2600:7d4a:2f07:955c:cd4f  64(good)  300(good)

ariyaps-iPad     192.168.1.122  a4:d1:d2:5f:32:52  iPad     SG1    BLDG-A-ATV1        149      AN
SG1            fd14:5f94:8156:2600:8e1:313a:3231:2cf5   39(good)  39(good)

Apple-TV-5       192.168.1.118  9c:20:7b:ab:b5:71           SG1    BLDG-A-ATV1        149      AN
AppleTV        fd14:5f94:8156:2600:8d9:6a60:9da6:3d5b   43(good)  39(good)

Number of Clients   :4
Info timestamp      :332031
BLDG-A-ATV1#
```

And when we ping from Client-1 to client-2, the ping is successful as it can be seen here.

```
BLDG-A-ATV1# sh datap session | incl 192.168.1.129
192.168.1.122     192.168.1.129   1    9     0     0    0    0   1   dev8        5c   0       0
FYI
192.168.1.122     192.168.1.129   1    11    0     0    0    0   0   dev8        2c   1       3c
FI
192.168.1.122     192.168.1.129   1    10    0     0    0    0   1   dev8        45   0       0
FYI
192.168.1.122     192.168.1.129   1    12    0     0    0    0   0   dev8        27   1       3c
FI
192.168.1.129     192.168.1.122   1    11    2048  0    0    0   0   dev8        2c   0       0
FYCI
192.168.1.129     192.168.1.122   1    10    2048  0    0    0   1   dev8        45   0       0
FYCI
192.168.1.129     192.168.1.122   1    9     2048  0    0    0   1   dev8        5c   0       0
FYCI
192.168.1.129     192.168.1.122   1    12    2048  0    0    0   0   dev8        27   0       0
FYCI
BLDG-A-ATV1#
```

With “Deny Inter User Bridging”, one can discover devices on the same subnet, however you can use ACLs in the use roles to block traffic to/from other subnets.

3.2 Client Isolation Configuration

To start off with, we’ll turn off “Deny Inter User Bridging” on SG1. The new command is “deny-intra-vlan-traffic” that needs to be applied to the SSID profile.

```
BLDG-A-ATV1# conf t
We now support CLI commit model, please type "commit apply" for configuration to take
effect.
BLDG-A-ATV1 (config) # wlan ssid-profile SG1
BLDG-A-ATV1 (SSID Profile "SG1") # deny-intra-vlan-traffic
```

```
BLDG-A-ATV1 (SSID Profile "SG1") #
BLDG-A-ATV1# com app
committing configuration...
configuration committed.
BLDG-A-ATV1#
```

So now when we ping from Client-1 to Client-2, the ping fails and there is nothing in the datapath

```
BLDG-A-ATV1# sh datapath session | incl 192.168.1.129
BLDG-A-ATV1# sh datapath session | incl 192.168.1.129
BLDG-A-ATV1#
```

When we configured “deny-intra-vlan-traffic” command, the Instant cluster will learn the IP address and its subnet, MAC address of the default gateway and DNS and created a “trusted” table that it can refer to.

Here is that trusted table, you can see there are two entries and it has already picked up the default gateway which happen to be the DNS as well.

```
BLDG-A-ATV1# sh datapath subnet

Flags: L - Local, G - Gateway, D - DNS, S - Static

Subnet Datapath Table
---------------------
VLAN  IP           MASK           MAC                IP Age  MAC Age  Flags
----  --           ----           ---                ------  -------  -----
1     192.168.1.1  255.255.255.0  14:5f:94:81:56:26  0       0        GD
3333  172.31.98.1  0.0.0.0        20:4c:03:23:a7:c0  0       0        LG
BLDG-A-ATV1#
```

You can add to this trusted subnet table or the whitelist. Here we have a printer (192.168.1.249) on this subnet that needs to be reachable from the clients. Again without adding to the whitelist, the printer is not reachable by Client-1 and Client-2

There is a new profile to this whitelist and its “intra-vlan-traffic-profile”. Here we’ll add the printer’s IP address or MAC address to the list.

```
BLDG-A-ATV1# conf t
We now support CLI commit model, please type "commit apply" for configuration to take
effect.
BLDG-A-ATV1 (config) # intra-vlan-traffic-profile
BLDG-A-ATV1 (intra-vlan-traffic) # wired-server-ip 192.168.1.249
BLDG-A-ATV1 (intra-vlan-traffic) # wired-server-mac b0:5a:da:98:b5:70
BLDG-A-ATV1 (intra-vlan-traffic) #
BLDG-A-ATV1# com app
committing configuration...
configuration committed.
BLDG-A-ATV1#
BLDG-A-ATV1# sh datapath subnet

Flags: L - Local, G - Gateway, D - DNS, S - Static

Subnet Datapath Table
---------------------
VLAN  IP             MASK           MAC                IP Age  MAC Age  Flags
```

```
----  --              ----            ---                 ------  -------  -----
1     192.168.1.1     255.255.255.0   14:5f:94:81:56:26   0       0        GD
1     192.168.1.249   255.255.255.0   b0:5a:da:98:b5:70   0       0        S
3333  172.31.98.1     0.0.0.0         20:4c:03:23:a7:c0   0       0        LG
BLDG-A-ATV1#
```

Now we can successfully ping 192.168.1.249 from client-1 and 2.

```
20:4c:03:23:a7:98# sh datap sess | incl 192.168.1.129
192.168.1.249     192.168.1.129   1    185   0     0    0    56  1   dev25       8    1
3c    FI
192.168.1.249     192.168.1.129   1    184   0     0    0    56  1   dev25       d    1
3c    FI
192.168.1.249     192.168.1.129   1    183   0     0    0    56  1   dev25       11   0
0     FI
192.168.1.249     192.168.1.129   1    182   0     0    0    56  1   dev25       17   0
0     FI
192.168.1.129     192.168.1.249   1    185   2048  0    0    0   0   dev25       8    0
0     FYCI
192.168.1.129     192.168.1.249   1    184   2048  0    0    0   0   dev25       d    0
0     FYCI
192.168.1.129     192.168.1.249   1    183   2048  0    0    0   0   dev25       11   0
0     FYCI
192.168.1.129     192.168.1.249   1    182   2048  0    0    0   0   dev25       17   0
0     FYCI

20:4c:03:23:a7:98#
```

If you wanted to add the MAC addresses to the subnet table, the command is

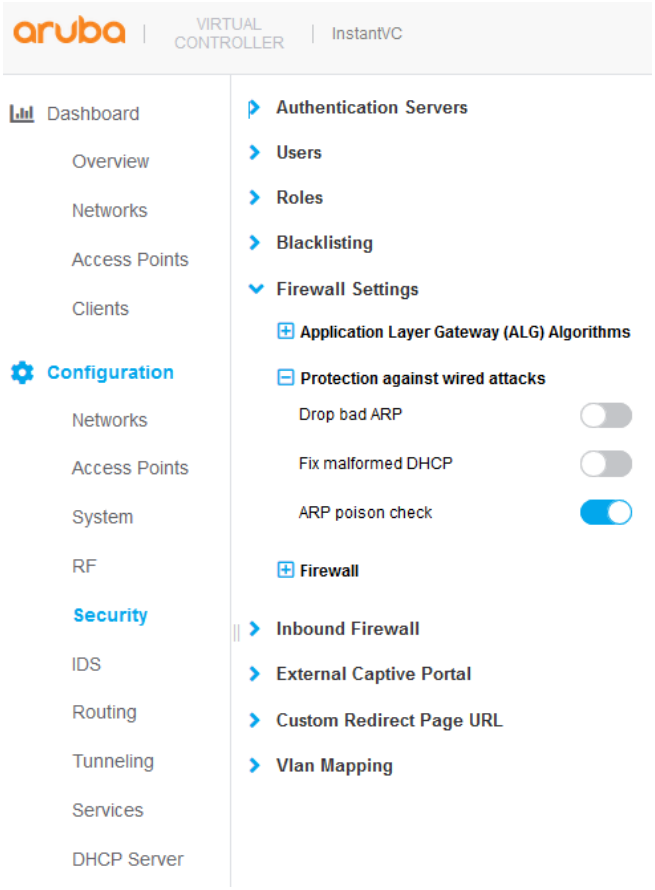
“`wired-server-mac <MAC address>`”

Few points to note

- Client isolation is used only for IPv4 and does not support Airgroup features
- You can have max of 32 wired server IP addresses
- You can only add wired IP/MAC addresses to the trusted subnet table

It is highly recommended to enable ARP poison check as well in which it triggers alerts when a known client on the Instant AP spoofs the base MAC address of the Instant AP.

You can configure it as shown below.


aruba | VIRTUAL CONTROLLER | InstantVC
Dashboard
Overview
Networks
Access Points
Clients
Configuration
Networks
Access Points
System
RF
Security
IDS
Routing
Tunneling
Services
DHCP Server
Authentication Servers
Users
Roles
Blacklisting
Firewall Settings
Application Layer Gateway (ALG) Algorithms
Protection against wired attacks
Drop bad ARP
Fix malformed DHCP
ARP poison check
Firewall
Inbound Firewall
External Captive Portal
Custom Redirect Page URL
Vlan Mapping