Controller Type: **200**

Controller Image Version: **ArubaOS 5.0.4.11**

Controller IP Address: **192.168.2.222**

RAP Type: **RAP-2WG**

RAP IP Address: **192.168.2.125 (Assigned by external DHCP Server)**

**(ICI) #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

CHAP

MSCHAP

MSCHAPv2

EAP

IP LOCAL POOLS:

RAP-Pool: 10.10.123.100 - 10.10.123.200

**(ICI) #show crypto isakmp key**

ISAKMP Local Pre-Shared keys configured for ANY FQDN

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

Key

---

ISAKMP Local Pre-Shared keys configured by FQDN

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

FQDN of the host Key

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

ISAKMP Local Pre-Shared keys configured by Address

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

IP address of the host Subnet Mask Length Key

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

ISAKMP Global Pre-Shared keys configured by Address

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

IP address of the host Subnet Mask Length Key

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

10.10.123.0 24 \*\*\*\*\*\*\*\*

**(ICI) #show crypto ipsec transform-set**

Transform set default-transform: { esp-3des esp-sha-hmac }

will negotiate = { Transport, Tunnel }

Transform set default-ml-transform: { esp-3des esp-sha-hmac }

will negotiate = { Transport, Tunnel }

Transform set default-cluster-transform: { esp-aes256 esp-sha-hmac }

will negotiate = { Transport, Tunnel }

**(ICI) (config) #show ap database**

AP Database

-----------

Name Group AP Type IP Address Status Flags Switch IP

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

00:24:6c:cd:59:a6 default RAP-2WG 192.168.2.125 Down 192.168.2.222

Flags: U = Unprovisioned; N = Duplicate name; G = No such group; L = Unlicensed

I = Inactive; H = Using 802.11n license

X = Maintenance Mode; P = PPPoE AP; B = Built-in AP

R = Remote AP; R- = Remote AP requires Auth; C = Cellular RAP; c = CERT-based RAP

M = Mesh node; Y = Mesh Recovery

Total APs:1

**(ICI) (config) #show datapath session table 192.168.2.125 | include 4500**

192.168.2.222 192.168.2.125 17 4500 49159 0/0 0 0 2 1/1 19 F

192.168.2.125 192.168.2.222 17 49159 4500 0/0 0 0 1 1/1 19 FC

**(ICI) (config) #show datapath session table 192.168.2.125 | include 4500**

192.168.2.222 192.168.2.125 17 4500 49159 0/0 0 0 2 1/1 20 F

192.168.2.222 192.168.2.125 17 4500 49161 0/0 0 0 0 1/1 7 F

192.168.2.125 192.168.2.222 17 49159 4500 0/0 0 0 1 1/1 20 FC

192.168.2.125 192.168.2.222 17 49161 4500 0/0 0 0 0 1/1 7 FC

**(ICI) (config) # show crypto isakmp sa**

% No active ISAKMP SA

**(ICI) (config) #show datapath session table 192.168.2.125**

Datapath Session Table Entries

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

Flags: F - fast age, S - src NAT, N - dest NAT

D - deny, R - redirect, Y - no syn

H - high prio, P - set prio, T - set ToS

C - client, M - mirror, V - VOIP

I - Deep inspect, U - Locally destined

Source IP Destination IP Prot SPort DPort Cntr Prio ToS Age Destination TAge Flags

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

192.168.2.125 192.168.2.222 17 49152 514 0/0 0 0 0 1/1 28 FC

192.168.2.222 192.168.2.125 17 514 49152 0/0 0 0 2 1/1 28 FY

192.168.2.254 192.168.2.125 1 0 0 0/0 0 0 1 1/0 28 FC

192.168.2.255 192.168.2.125 1 0 0 0/0 0 0 2 1/1 28 FYI

192.168.2.252 192.168.2.125 1 0 0 0/0 0 0 1 1/0 28 FC

192.168.2.253 192.168.2.125 1 0 0 0/0 0 0 1 1/0 28 FC

192.168.2.222 192.168.2.125 1 0 0 0/0 0 0 1 local 28 FC

192.168.2.201 192.168.2.125 1 0 0 0/0 0 0 1 1/0 28 FC

192.168.2.10 192.168.2.125 1 0 0 0/0 0 0 1 1/0 28 FC

192.168.2.125 192.168.2.255 1 0 2048 0/0 0 0 1 1/1 28 FCI

192.168.2.222 192.168.2.125 17 4500 49163 0/0 0 0 1 1/1 e F

192.168.2.222 192.168.2.125 17 4500 49161 0/0 0 0 2 1/1 27 F

192.168.2.125 192.168.2.222 17 49163 4500 0/0 0 0 0 1/1 e FC

192.168.2.125 192.168.2.222 17 49161 4500 0/0 0 0 1 1/1 27 FC

**(ICI) (config) #show log security 30**

Feb 8 17:31:54 :103063: <DBUG> |ike| Aruba RAP detected

Feb 8 17:31:54 :103063: <DBUG> |ike| IKE Fragmentation

Feb 8 17:31:54 :103063: <DBUG> |ike| message\_recv enabling early NATT since peer initiates on 4500

Feb 8 17:31:54 :103060: <DBUG> |ike| ike\_phase\_1.c:ike\_phase\_1\_responder\_recv\_SA:905 Recvd VPN IKE Phase 1 SA transform negotiation (1st packet) from IP 192.168.2.125.

Feb 8 17:31:54 :103060: <DBUG> |ike| ike\_phase\_1.c:ike\_phase\_1\_responder\_recv\_SA:934 Found our AP vendor ID from external IP 192.168.2.125

Feb 8 17:31:54 :103060: <DBUG> |ike| ike\_phase\_1.c:attribute\_unacceptable:2907 Proposal match failed in auth algo, configured=RSA\_SIG, peer using=unknown

Feb 8 17:31:54 :103060: <DBUG> |ike| ike\_phase\_1.c:attribute\_unacceptable:2929 Proposal match failed in key length, configured=32, peer using=16

Feb 8 17:31:54 :103060: <DBUG> |ike| ike\_phase\_1.c:attribute\_unacceptable:2889 Proposal match failed in hash algo, configured=SHA, peer using=MD5

Feb 8 17:31:54 :103060: <DBUG> |ike| ike\_phase\_1.c:attribute\_unacceptable:2907 Proposal match failed in auth algo, configured=RSA\_SIG, peer using=unknown

Feb 8 17:31:54 :103060: <DBUG> |ike| ike\_phase\_1.c:attribute\_unacceptable:2929 Proposal match failed in key length, configured=32, peer using=24

Feb 8 17:31:54 :103060: <DBUG> |ike| ike\_phase\_1.c:attribute\_unacceptable:2889 Proposal match failed in hash algo, configured=SHA, peer using=MD5

Feb 8 17:31:54 :103060: <DBUG> |ike| ike\_phase\_1.c:attribute\_unacceptable:2907 Proposal match failed in auth algo, configured=RSA\_SIG, peer using=unknown

Feb 8 17:31:54 :103060: <DBUG> |ike| ike\_phase\_1.c:ike\_phase\_1\_responder\_recv\_SA:1049 Ike Phase 1 received SA

Feb 8 17:31:54 :103063: <DBUG> |ike| ike\_phase\_1\_responder\_send\_SA\_NAT\_T Accepted 1 of the Proposals, sending Response for exchange:192.168.2.125

Feb 8 17:31:55 :103063: <DBUG> |ike| nat\_t\_exchange\_check\_nat\_d\_has\_us src-port:500 dst-port:49165

Feb 8 17:31:55 :103060: <DBUG> |ike| nat\_traversal.c:nat\_t\_generate\_nat\_d\_hash:267 IP 192.168.2.222 Port 500

Feb 8 17:31:55 :103060: <DBUG> |ike| nat\_traversal.c:nat\_t\_exchange\_check\_nat\_d\_has\_us:561 Did not find our matching NAT-D payload for Port:500 in their packet

Feb 8 17:31:55 :103060: <DBUG> |ike| nat\_traversal.c:nat\_t\_generate\_nat\_d\_hash:267 IP 192.168.2.222 Port 4500

Feb 8 17:31:55 :103060: <DBUG> |ike| nat\_traversal.c:nat\_t\_exchange\_check\_nat\_d\_has\_us:571 Found our matching NAT-D payload for Port:4500 in their packet

Feb 8 17:31:55 :103060: <DBUG> |ike| nat\_traversal.c:nat\_t\_generate\_nat\_d\_hash:267 IP 192.168.2.125 Port 49165

Feb 8 17:31:55 :103060: <DBUG> |ike| nat\_traversal.c:nat\_t\_generate\_nat\_d\_hash:267 IP 192.168.2.222 Port 4500

Feb 8 17:31:55 :103060: <DBUG> |ike| nat\_traversal.c:nat\_t\_exchange\_add\_nat\_d:377 NAT-T added hashes for src=192.168.2.222:4500, dst=192.168.2.125:4500

Feb 8 17:31:55 :103063: <DBUG> |ike| ike\_phase\_1\_send\_KE\_NONCE 192.168.2.125

Feb 8 17:31:55 :103063: <DBUG> |ike| GetFirstMatchIsakmpPSK: entering

Feb 8 17:31:55 :103063: <DBUG> |ike| mask FFFFFF00, ip C0A8027D, key\_ip A0A7B00

Feb 8 17:31:55 :103004: <INFO> |ike| No ISAKMP PSK found for peer 192.168.2.125

Feb 8 17:31:55 :103063: <DBUG> |ike| ipsec\_get\_keystate: no keystate in ISAKMP SA 0x102eb2c4

Feb 8 17:31:55 :103060: <DBUG> |ike| message.c:message\_recv:1948 freeing message : no keystate to decrypt this packet

Feb 8 17:31:58 :103063: <DBUG> |ike| ipsec\_get\_keystate: no keystate in ISAKMP SA 0x102eb2c4

Feb 8 17:31:58 :103060: <DBUG> |ike| message.c:message\_recv:1948 freeing message : no keystate to decrypt this packet