IAP VPN Configuration
Central 2.5.0
Miscellaneous Details

- Aruba Central version is 2.5.0
- VPNC is pre-configured for OTO and RTO configuration which are not shown in this document
- In current Setup VPNC is running OSPF with Datacenter Core Switch and OSPF configurations are not included in this document only the IAP VPN Overlay routing redistribution into OSPF are covered
- This guide assume that VPNC is already configured with necessary VLANs, WAN links, IP address and IPsec etc...hence not covered in this document
VPNC Configuration

- If VPNC and BGW are under the same Central account then no need to configure any authentication
- Navigate to VPN -> General VPN and add the Address Pool
- These range of IP address will be allocated to the IAP over L2TP
- Also select option “IAP-VPN backward compatible:”
VPNC Configuration

- Navigate to Routing -> OSPF -> Redistribution add the source protocol as “IAP-VPN overlay” to advertise the IAP VPN LAN subnets to Core Switch via OSPF.
VPNC Configuration

• Navigate to Security -> L3 Authentication -> VPN Authentication -> default-iap and make sure Default role “default-vpn-role” should be selected
• Navigate to Security -> Roles and expand role name “default-vpn-role”, go to Tab “More” and under VPN-> L2tp pool select “iap_vpn” which was created earlier.
• However without selecting the “iap_vpn” pool IAP VPN still working in current setup
IAP Configuration at Group level

- Configure the SSID as per requirement
IAP Configuration at Group level

• Configure Security level as per requirement
IAP Configuration at Group level

• It is mandatory to configure the either Distributed DHCP Scope or Centralized DHCP Scope then only the branch subnets can be advertised to VPNC. This setup is configured for Distributed DHCP Scope with type as “Distributed,Layer3”. There is no need to configure IP address for VLAN11. The IP address and default gateway will be allocated by DHCP Server

• Navigate System -> DHCP ->Distributed DHCP Scope and click “+”
IAP Configuration at Group level

- Navigate VPN -> VPN and add the Public IP address of VPNC as Primary Host, select Protocol as “Aruba IPsec”
- Navigate VPN -> Routing and add the static route for Data Center
Show Command at VPNC

- Run the below commands to validate

**(VPNC1) */#show iap table**

Trusted Branch Validation: Enabled  
IAP Branch Table  
------------------
Name       VC MAC Address     Status  Inner IP     Assigned Subnet  Assigned Vlan  
---------  --------------     ------  ----------     --------------     ------
- AP205_VPN  94:b4:0f:cb:76:3a  UP      20.20.20.23  11.11.11.32/27
  
Total No of UP Branches : 1  
Total No of DOWN Branches : 0  
Total No of Branches      : 1

**(VPNC1) */#show crypto IPsec Sa**

IPSEC SA (V2) Active Session Information  
--------------------------------------
Initiator IP                              Responder IP                              SPI(IN/OUT)        Flags Start Time  Inner IP  
---------  --------------     --------------     ------  ------------------     ----------
223.190.59.180                            192.168.253.5                             aecfa000/792b1b00 UT2   Feb 25 20:48:06  20.20.20.23
Show Command at VPNC

- Run the command to validate

(VPNC1) *#show ip route

Codes: C - Connected, O - OSPF, IA - OSPF Inter Area, E1 - OSPF External Type 1
        E2 - OSPF External Type 2, B I - BGP Interior, B E - BGP Exterior, S - Static
        U - BGW Peer Uplink, M - Management, Ru - Route Usable, * - Candidate Default
        V - RAPNG VPN/Branch, I - Crypto-Cfgset, N - Not Redistributed, Bc - Cloud Overlay Protocol

S*  0.0.0.0/0   [50/1] via 192.168.253.1
O E2 192.168.0.0/24  [110/25] via 192.168.10.1
C  192.168.10.0/24 is directly connected, VLAN10
O E2 192.168.20.0/24  [110/25] via 192.168.10.1
O E2 192.168.30.0/24  [110/25] via 192.168.10.1
O E2 172.10.10.0/24  [110/25] via 192.168.10.1
O E2 20.20.93.0/24  [110/25] via 192.168.10.1
O E2 20.20.94.0/24  [110/25] via 192.168.10.1
Bc 10.90.100.0/24   [90/10] ipsec map default-vpnip-master-ipseccmap-20:4c:03:2f:f2:8c-inet2_inet
    [90/10] ipsec map default-vpnip-master-ipseccmap-20:4c:03:2f:f2:8c-inet1_inet
V  20.20.20.23/32   [60/10] via 20.20.20.23
C  192.168.253.0/29 is directly connected, VLAN4093
O  192.168.254.0/30  [110/101] via 192.168.10.1
V  11.11.11.32/27   [60/10] via 20.20.20.23
IAP Monitoring in Central

- Currently the Central Monitoring page for VPNC does not show the tunnel details.
- For tunnel details go to IAP Summary page. Select the Group -> Device-> Access Point and click on the IAP, which will take you to the summary page.
- In summary page click Tunnel and review the details.
VPNC Route Monitoring in Central

- For Routing details go to VPNC Summary page. Select the Group -> Device-> Gateways and click on the VPNC, which will take you to the summary page
- In summary page Under the Routing click “Routing Table” and review the routing table and see if 20.20.x.x and 11.11.x.x networks are available
**VPNC and IAP Version Details**

- Below are the version details of VPNC and IAP tested for IAP VPN

<table>
<thead>
<tr>
<th>NAME</th>
<th>MAC ADDRESS</th>
<th>MODEL</th>
<th>FIRMWARE VERSION</th>
<th>RECOMMENDED VERSION</th>
<th>UPGRADE STATUS</th>
<th>COMPLIANCE STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPNC1</td>
<td>00:1a:1e:04:95:30</td>
<td>A7210</td>
<td>8.4.0.0-1.0.6.2.72991</td>
<td>8.4.0.0-1.0.6.2.72991</td>
<td>Firmware up to date</td>
<td>Not Set</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAME</th>
<th>APS</th>
<th>FIRMWARE VERSION</th>
<th>RECOMMENDED VERSION</th>
<th>UPGRADE STATUS</th>
<th>COMPLIANCE STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP205_VPN</td>
<td>1</td>
<td>6.5.4.16.74160</td>
<td>6.5.4.15.73677</td>
<td>Firmware up to date</td>
<td>Not Set</td>
</tr>
</tbody>
</table>
Thank You