VIA 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
• This guide assume that the VPNC is already configured with necessary VLANs, WAN links, IP address and IPsec etc…hence not covered in this document
• CPPM is used to authenticate the VIA clients and has simple radius services configured with enforcement as “Allow Access Profile”
VPNC Configuration

- Navigate to VPN -> General VPN and add the Address Pool name “via_vpn”
- These range of IP address will be allocated to the VIA client over L2TP
- Also select the option “Source-nat” and “VIA SSL failback”
- Add the corporate DNS, here we are using 8.8.8.8
VPNC Configuration

- Navigate to Routing -> VPN-> Shared Secrets and add key as “aruba123” rest all filed blank
VPNC Configuration

- Navigate to Security -> Auth Server and add Server Group as “cppm”
- Click on the server group “cppm” to expand and add server as “cppm”, IP address of Clearpass server and Shared key as “aruba123”
VPNC Configuration

- Navigate Security -> L3 Authentication -> VIA Authentication and add new VIA Authentication Profile name “VIA_CPPM_Auth”
- Under the newly created profile select CPPM in “Radius Accounting Server Group” and “Server Group”
VPNC Configuration

- Navigate Security -> L3 Authentication -> VIA Connection and add new VIA Connection Profile name “via_connection”
- Under the newly created profile add VIA Server (Public and Private IP address of VPNC) and VIA authentication profile to provision as “VIA_CPPM_Auth”
- Add VIA Tonneled networks as Datacenter subnets reachable to VIA clients
- Enable split Tunnel if required rest all settings can be default
VPNC Configuration

• Navigate Security-> L3 Authentication -> VIA Authentication and click previously created profile “VIA_CPPM_Auth”
• Refer the Default Role assigned which is “default-via-role” you can assign user defined role as well
• Navigate to Security -> Roles and expand role name “default-via-role”, go to Tab “More” and under VPN-> L2tp pool select “iap_vpn” and VIA connection profile as “via_connection” which was created earlier.
CPPM Configuration

- Navigate Configuration > Network -> Devices and click “Add” and provide the IP address of the VPNC and Shared Key defined in slide 5
- Apparently VPNC uses WAN IP address to send the radius request to CPPM
CPPM Configuration

- Navigate Configuration > Services and click “Add” and create the service as below
- Navigate Configuration > Identity -> Local Users and click “Add” and create a user account
VIA Client Configuration

- Install the latest version of VIA on windows machine
- Open VIA and provide the IP address of VPNC and click Download
- If the connection to VPNC is reachable, the VIA client will ask for the username and password
- VIA uses port 443 so make sure your firewall is allowing that port
- After the authentication VIA will download the profile from VPNC and establish the secure connection
Show Command at VPNC

- Run the below commands to validate

(VPNC1) *#show crypto ipsec sa

IPSEC SA Active Session Information
-----------------------------------
Initiator IP  Responder IP  InitiatorID  ResponderID  Flags  Start Time  Inner IP
---------  ---------  ---------  ---------  -----  ------------  -------
223.190.59.180  192.168.253.5  30.30.33/32  0.0.0.0/0  UT  Feb 27 18:33:16  30.30.33

Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap
L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2
l = uplink load-balance t = Tunnel Service

Total IPSEC SAs: 1

(VPNC1) *#show user

This operation can take a while depending on number of users. Please be patient ....

Users
-----
---------  ---------  -----  -------  -----  ------  ------------  -------  -----  ------
30.30.33  00:00:00:00:00:00  viavpn  default-via-role  00:00:05  VIA-VPN  223.190.59.180  N/A
223.190.59.180  00:00:00:00:00:00  logon  VIA-VPN  223.190.59.180  N/A

User Entries: 2/2
Curr/Cum Alloc:3/29 Free:0/26 Dyn:3 AllocErr:0 FreeErr:0
VPNC and IAP Version Details

- Below are the version details of VPNC and VIA under test

<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:04:5d:0d</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>
Thank You